# Whitehead Group of the Iwasawa algebra of GL2(Zp)

Solanki, Vishal

*Awarding institution:*
King's College London

# Whitehead Group of the Iwasawa algebra of $GL_2(\mathbb{Z}_p)$

Vishal Solanki
Doctor Of Philosophy in Mathematics

June 30, 2018

**Abstract**

Main conjectures in Iwasawa theory are interesting because they give a deep connection between arithmetic and analytic objects in number theory. One of the most important recent developments in Iwasawa theory is the formulation of non-commutative main conjectures by Coates, Fukaya, Kato, Sujatha and Venjakob using $K_1$ groups. Burns and Kato supplied a strategy to prove these non-commutative main conjectures. After important special cases were proved by Kato and Hara, the non-commutative main conjecture for totally real fields was proved by Kakde using this strategy (it was proved independently by Ritter-Weiss). In this thesis we imitate Kakde's computation of $K_1$ groups in order to obtain a description of the $K_1$ group of the Iwasawa algebra of $GL_2(\mathbb{Z}_p)$. While we do not find an explicit description of this group, we do define another group which must contain this $K_1$ group.

# Contents

# Chapter 1

# Introduction

In this thesis we describe the Whitehead group or the first $K$-group, $K_1$, of the Iwasawa algebra of $GL_2(\mathbb{Z}_p)$ for odd prime $p$. We are interested in this $K_1$ group because of its appearance in non-commutative Iwasawa theory for elliptic curves without complex multiplication[1]. Let $E$ be an elliptic curve defined over $\mathbb{Q}$. Put $K_\infty = \bigcup_{n\geq 1} \mathbb{Q}(E[p^n])$ and $\mathcal{G} = Gal(K_\infty/\mathbb{Q})$. If $E$ admits complex multiplication by an order in an imaginary quadratic field $F$, then $Gal(K_\infty/F)$ is abelian. In this case a main conjecture for $E$ and the extension $K_\infty/F$ can be formulated using the structure theory for finitely generated modules over the Iwasawa algebra of $K_\infty/F$. Indeed this main conjecture was proved in Rubin ([16] , [22]).

On the other hand, if $E$ does not admit complex multiplication, then by a celebrated theorem of Serre [18], $\mathcal{G}$ is an open subgroup of $GL_2(\mathbb{Z}_p)$. In fact, for all sufficiently large prime $p$, $\mathcal{G}$ is equal to $GL_2(\mathbb{Z}_p)$. However, the whole approach of classical Iwasawa theory breaks down due to lack of good structure theory for finitely generated modules over the Iwasawa algebra of $GL_2(\mathbb{Z}_p)$. Venjakob [20] and Coates, Fukaya, Kato, Sujatha and Venjakob [4] bypassed structure theory by formulating the main conjecture using algebraic $K$-theory. Thus it is essential to study $K_1$ groups of Iwasawa algebras of non-commutative $p$-adic Lie groups. Kato's seminal paper [13] provided a strategy for computing $K_1$ of the Iwasawa algebra of a $p$-adic Lie group $G$ using Iwasawa algebras of abelian sub-quotients of $G$ by working out a specific example of $G \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$. This result was generalised independently by Kakde [11] and Ritter-Weiss ([15], [21]) after special cases were worked out by Kato [13], Kakde [10] and Hara ([8], [9]). These computations of $K_1$ groups of Iwasawa algebras and certain localisations show that, in order to prove the non-commutative main conjecture, we must prove "several" commutative main conjectures and prove certain congruences between commutative $p$-adic $L$-functions (such a strategy usually assumes vanishing of certain $\mu$-invariant but we will not discuss this here). This is the so called Burns-Kato strategy for proving the non-commutative main conjecture.

The computation of $K_1$ by Ritter-Weiss requires working with all abelian sub-quotients. The computation of $K_1$ by Kato, generalized by Kakde, has an advantage that we do not necessarily need all abelian sub-quotients. In this thesis we use this observation and describe $K_1$ of the Iwasawa algebra of $GL_2(\mathbb{Z}_p)$ by using abelian sub-quotients which come from "well-known" subgroups such as Borel, Cartan, etc.

[1] An elliptic curve $E$ admits **complex multiplication** if it has an endomorphism ring larger than the integers; the endomorphism ring is a set of complex numbers which map the lattice, of the elliptic curve, to a subset of the lattice. An elliptic curve with complex multiplication is one with endomorphism ring isomorphic to an imaginary quadratic extension of the integers.

Let us now describe our results in more detail. From now on we assume $p$ is odd.

## 1.1 The strategy of Burns and Kato

Let $\mathcal{G}$ be a $p$-adic Lie group. We put $\Lambda(G) = \mathbb{Z}_p[[G]] := \varprojlim_U \mathbb{Z}_p[G/U]$, for a pro-finite group $G$, where $U$ runs through open normal subgroups of $G$. If $U$ is an open subgroup of $\mathcal{G}$ and $V$ is a closed normal subgroup of $U$ such that $U/V$ is abelian, then there are maps

$$\theta_{U,V} : K_1(\Lambda(\mathcal{G})) \to K_1(\Lambda(U)) \to K_1(\Lambda(U/V)) \cong \Lambda(U/V)^\times$$

where the first map is the norm map[2]and the second map is induced by the natural projection $\Lambda(U)) \to \Lambda(U/V)$. Now let $\mathcal{F}$ be a collection of pairs $(U, V)$ as above. Then we have a map:

$$\theta_{\mathcal{F}} = \prod_{(U,V)\in\mathcal{F}} (\theta_{(U,V)})_{(U,V)\in\mathcal{F}} : K_1(\Lambda(\mathcal{G})) \to \prod_{(U,V)\in\mathcal{F}} \Lambda(U/V)$$

The idea is to study the kernel and the image of $\theta_{\mathcal{F}}$.

## 1.2 Our choice of $\mathcal{F}$ for $GL_2(\mathbb{Z}_p)$

We use the isomorphism

$$GL_2(\mathbb{Z}_p) = \varprojlim_n GL_2(\mathbb{Z}/p^n\mathbb{Z})$$

Using a result of Fukaya-Kato ([7], see ([11], Lemma 4.1)) we get

$$K_1(\Lambda(GL_2(\mathbb{Z}_p))) \cong \varprojlim_n K_1(\mathbb{Z}_p[GL_2(\mathbb{Z}/p^n\mathbb{Z})])$$

We therefore study $K_1$ of the group ring $\mathbb{Z}_p[GL_2(\mathbb{Z}/p^n\mathbb{Z})]$. Consider the set of subgroups of $GL_2(\mathbb{Z}/p^n\mathbb{Z})$ (these subgroups are defined in Chapter 3):

$$\mathcal{F}_n = \{Z_n, C_n, T_n, K_n, N_{t^i}, N_{k^i} | \forall i = 1, 2, ..., n-1\}$$

Consider the map

$$\theta_n = \prod_{U\in\mathcal{F}_n} (\theta_{(U,[U,U])})_{U\in\mathcal{F}_n} : K_1(\mathbb{Z}_p[GL_2(\mathbb{Z}/p^n\mathbb{Z})]) \to \prod_{U\in\mathcal{F}_n} \mathbb{Z}_p[U^{ab}]^\times$$

In fact, all subgroups in $\mathcal{F}_n$ are abelian already, so $\mathbb{Z}_p[U^{ab}]^\times = \mathbb{Z}_p[U]^\times$ for each $U \in \mathcal{F}_n$.

In Chapter 5 we prove that image of $\theta_n$ is contained in an explicitly defined subgroup $\Theta_{n,\mathbb{Z}_p}$ of $\prod_{U\in\mathcal{F}_n} \mathbb{Z}_p[U]^\times$ (see Theorem 5.1). Unfortunately, we are unable to show that the image of $\theta_n$ is exactly $\Theta_{n,\mathbb{Z}_p}$. This is due to our lack of knowledge of the kernel and cokernel of the map $\mathcal{L}$ defined in Chapter 5. We also prove a similar result about twisted group rings $R[GL_2(\mathbb{Z}/p^n\mathbb{Z})]^\tau$ for a specific ring $R$. This twisted group ring is the localisation of the Iwasawa algebra of a one dimensional quotient of $GL_2(\mathbb{Z}_p)$ at the canonical Ore set of Coates, Fukaya, Kato, Sujatha and Venjakob (for details see Section 2.1).

[2]To define this norm, we first notice that $\Lambda(\mathcal{G})$ is a free $\Lambda(U)$-module of rank $d = [\mathcal{G} : U]$, i.e. $\Lambda(\mathcal{G}) \cong \Lambda(U)^d$. So there is a map $GL_n(\Lambda(\mathcal{G})) \to GL_{nd}(\Lambda(U))$ which induces the norm map $K_1(\Lambda(\mathcal{G})) \to K_1(\Lambda(U))$.

## 1.3 Application of our results to Iwasawa theory

The main result (Theorem 5.1) states the following:

*The image of $\theta_n$ is contained in $\Theta_{n,\mathbb{Z}_p}$ which is defined using the following conditions:*

1. $\Theta_{n,\mathbb{Z}_p} \subset \prod_{U\in\mathcal{F}_n} \mathbb{Z}_p[U]^\times$ *such that* $x_{Z_n}^p \left(\lambda_{\mathcal{L},Z_n}((x_V)_{V\in\mathcal{F}_n})\right) \equiv \varphi(x_{Z_n}) \ (mod\ p^{3n-1})$
2. *For any* $(x_V)_{V\in\mathcal{F}_n} \in \Theta_{n,\mathbb{Z}_p}$, *each* $x_V$ *is fixed by conjugation action of* $N_{G_n}(V)$
3. *For any* $(x_V)_{V\in\mathcal{F}_n} \in \Theta_{n,\mathbb{Z}_p}$, *we have:*
   - $Nm_{V/Z_n}(x_V) = x_{Z_n}$ *for all* $V \in \mathcal{F}_n$
   - $\frac{1}{p}log\left(Nm_{U/Z_m\cap U}\left(\frac{x_U^p \varphi(N_U(x_U))^{p^2}\lambda_{\mathcal{L},U}((x_V))}{\varphi(x_U)^{p^2}\varphi(N_U(x_U))\nu_{\mathcal{L},U}(x_{C_n})}\right)\right) + Tr_{U/Z_m\cap U}\left(\mu_{\mathcal{L},U}(x_U)\sum_{\beta\in(\mathbb{Z}/p^i\mathbb{Z})^\times} rc_{1,\beta}^{n-i}\right)$ $= \frac{1}{p}log\left(Nm_{C_n/Z_m\cap C_n}\left(\frac{x_{C_n}^p N_{C_n}(\varphi(x_{C_n}))^p \lambda_{\mathcal{L},C_n}((x_V))}{\varphi(x_{C_n})^p\varphi\left(N_{C_n}(x_{C_n})\right)}\right)\right)$ *for* $U \in \{N_{t^i}, N_{k^i}\}$ *and* $m \geq n-i$
4. *For any* $(x_V)_{V\in\mathcal{F}_n} \in \Theta_{n,\mathbb{Z}_p}$, *we have:*
   - $Nm_{C_n/Z_m\cap C_n}\left(x_{C_n}^p N_{C_n}(\varphi(x_{C_n}))^p \left(\lambda_{\mathcal{L},C_n}((x_V)_{V\in\mathcal{F}_n})\right)\right)$ $\equiv Nm_{C_n/Z_m\cap C_n}\left(\varphi(x_{C_n})^p\varphi\left(N_{C_n}(x_{C_n})\right)\right)\ (mod\ p^{3m+1})$
   - $Nm_{U/Z_m\cap U}\left(x_U^p N_U(\varphi(x_U))\left(\lambda_{\mathcal{L},U}((x_V)_{V\in\mathcal{F}_n})\right)\right)$ $\equiv Nm_{U/Z_m\cap U}\left(\varphi(x_U)\varphi(N_U(x_U))\right)\ (mod\ p^{3m})$ *for* $U \in \{T_n, K_n\}$
   - $Nm_{U/Z_m\cap U}\left(x_U^p \varphi(N_U(x_U))^{p^2}\left(\lambda_{\mathcal{L},U}((x_V)_{V\in\mathcal{F}_n})\right)\right)$ $\equiv Nm_{U/Z_m\cap U}\left(\varphi(x_U)^{p^2}\varphi(N_U(x_U))\left(\nu_{\mathcal{L},U}(x_{C_n})\right)\right)\ (mod\ p^{3m+1})$ *for* $U \in \{N_{t^i}, N_{k^i}\}$

*For the definition of the maps $\lambda_{\mathcal{L},U}$, $\mu_{\mathcal{L},N}$ and $\nu_{\mathcal{L},N}$, please refer to Definition 5.1.*

Our algebraic result predicts certain congruences between abelian $p$-adic $L$-functions of elliptic curves. Proving these congruences seems to be extremely hard at present. However, it may be possible to numerically verify these and thus provide evidence for the non-commutative main conjecture from [4].

# Chapter 2

# Preliminaries

## 2.1 Iwasawa algebras and some localisations

Let $p$ be an odd prime number and $G$ be a compact $p$-adic Lie group. We assume that $G$ contains a closed normal subgroup $H$ such that $G/H = \Gamma$ is isomorphic to $\mathbb{Z}_p$, the additive group of $p$-adic integers. Define $\Lambda(G)$ to be the Iwasawa algbra of $G$ with coefficients in $\mathbb{Z}_p$:

$$\Lambda(G) = \mathbb{Z}_p[[G]] := \varprojlim_U \mathbb{Z}_p[G/U]$$

where $U$ runs through open normal subgroups of $G$.

We recall the canonical Ore set of [4][1]:

$$\mathcal{T}' := \{\lambda \in \Lambda(G) \mid \Lambda(G)/\Lambda(G)\lambda \text{ is a finitely generated } \Lambda(H)\text{- module}\}$$

Following [4] put

$$\mathcal{T} := \bigcup_{i \geq 0} p^i \mathcal{T}'$$

It is proven in ([4], Theorem 2.4) that $\mathcal{T}'$ and $\mathcal{T}$ are multiplicatively closed subsets of $\Lambda(G)$, do not contain zero divisors and satisfies the Ore-conditions[2] (both left and right). Consequently we can localise $\Lambda(G)$ with respect to $\mathcal{T}'$ and $\mathcal{T}$ and obtain inclusions:

$$\Lambda(G) \hookrightarrow \Lambda(G)_{\mathcal{T}'} \hookrightarrow \Lambda(G)_{\mathcal{T}}$$

Our aim is to study $K_1(\Lambda(\mathcal{G}))$, $K_1(\Lambda(\mathcal{G})_{\mathcal{T}'})$ and $K_1(\Lambda(\mathcal{G})_{\mathcal{T}})$ for $\mathcal{G} = GL_2(\mathbb{Z}_p)$.

From now on we put $\mathcal{G} = GL_2(\mathbb{Z}_p)$ and $G_n = GL_2(\mathbb{Z}/p^n\mathbb{Z})$. We also put $H = SL_2(\mathbb{Z}_p)$ (Note that $\mathcal{G}/H \cong \mathbb{Z}_p^\times$).

To study the localisation $\Lambda(\mathcal{G})_{\mathcal{T}'}$ we write $\Lambda(\mathcal{G})$ as an inverse limit of Iwasawa algebras of one dimensional quotients of $\mathcal{G}$ and then show that the corresponding localisation of these Iwasawa algebras is easy to study.

[1] In [4] the Ore set are denoted by $S$ and $S^*$

[2] Ore-condition basically means that all right fractions with denominator in $\mathcal{T}$ can be written as left fractions with denominator in $\mathcal{T}$, and vice-versa.

Put $H_n = SL_2(\mathbb{Z}/p^n\mathbb{Z})$ and put $\widetilde{G_n}$ to be the quotient of $\mathcal{G}$ that makes the following diagram commute: In other words $\widetilde{G_n} = \mathcal{G}/ker(H \to H_n)$.

$$\begin{array}{ccccccccc} 1 & \to & H & \to & \mathcal{G} & \to & \mathbb{Z}_p^\times & \to & 1 \\ & & \downarrow & & \downarrow & & =\downarrow & & \\ 1 & \to & H_n & \to & \widetilde{G_n} & \to & \mathbb{Z}_p^\times & \to & 1 \end{array}$$

Then $\mathcal{G} \cong \varprojlim_n \widetilde{G_n}$.

**Lemma 2.1** *There exists an open central subgroup $\Gamma_n$ in $\widetilde{G_n}$ such that $\widetilde{G_n}/\Gamma_n \cong G_n$.*

*Proof:*
Let $K_n = ker(\mathcal{G} \to G_n)$, and let $\Gamma_n = K_n/ker(H \to H_n)$. By the third isomorphism theorem, $\widetilde{G_n}/\Gamma_n \cong \mathcal{G}/K_n \cong G_n$. Also notice that $\Gamma_n$ is central in $\widetilde{G_n}$ since is it isomorphic to $1 + p^n\mathbb{Z}_p$.

□

The lemma allows us to express the Iwasawa algebra $\Lambda(\widetilde{G_n})$ as a twisted group ring. We recall the definition of twisted group rings.

**Definition 2.1** *Let $R$ be a ring and $P$ be any finite group. Let*

$$\tau : P \times P \to R$$

*be a 2-cocycle*[3]*. Then the twisted group ring, denoted by $R[P]^\tau$, is a free $R$-module generated by $P$. Denote the image of $h \in P$ in $R[P]^\tau$ by $\overline{h}$. Therefore every element in $R[P]^\tau$ can be written as $\sum_{h\in P} r_h\overline{h}$. The addition is component-wise and the multiplication has the following twist*

$$\overline{h} \cdot \overline{h'} = \tau(h, h')\overline{hh'}$$

**Example:** For us the most important example of twisted group rings comes as follows:
Let $Q$ be a finite group with central subgroup $Z$ such that $Q/Z \cong P$. Choose a section $s : P \to Q$ (this need not be a homomorphism but the identity must map to the identity). Then $\tau : P \times P \to Z$ defined by

$$\tau(p_1, p_2) = s(p_1)s(p_2)s(p_1p_2)^{-1}$$

is a 2-cocycle. Then for any ring $A$ we have:

$$A[Z][P]^\tau \xrightarrow{\cong} A[Q]$$

$$\sum_{x\in P} a_x\overline{x} \mapsto \sum_{x\in P} a_x s(x)$$

where $a_x$ lies in $A[Z]$. This map is an isomorphism.
*Proof:*
The map is clearly bijective but we must still prove that it is a homomorphism:
$\sum_{x\in P} a_x\overline{x} \mapsto \sum_{x\in P} a_x s(x)$ and $\sum_{x\in P} b_x\overline{x} \mapsto \sum_{x\in P} b_x s(x)$.

$$\begin{array}{rcll} & (\sum_{x\in P} a_x\overline{x})(\sum_{x\in P} b_x\overline{x}) & & \\ = & \sum_{x\in P}\left(\sum_{x=yz} a_y b_z \tau(y,z)\right)\overline{x} & \mapsto & \sum_{x\in P}\left(\sum_{x=yz} a_y b_z \tau(y,z)\right)s(x) \\ & & = & \sum_{x\in P}\left(\sum_{x=yz} a_y b_z s(y)s(z)s(x)^{-1}\right)s(x)) \\ & & = & (\sum_{x\in P} a_x s(x))(\sum_{x\in P} b_x s(x)) \end{array}$$

□

[3] A map, $\tau$, is a 2-cocycle if it satisfies the condition $\tau(p_1, p_2)\tau(p_1p_2, p_3) = (\overline{p_1} * \tau(p_2, p_3))\,\tau(p_1, p_2p_3)$

**Lemma 2.2** *This is an isomorphism*

$$\mathbb{Z}_p[[\widetilde{G_n}]] \xrightarrow{\cong} \mathbb{Z}_p[[\Gamma_n]][G_n]^\tau$$

*Furthermore, we may choose $\tau$ such that, for any $A, B \in G_n$, $\tau(A, A^{-1}) = \mathbf{1}_2 = \tau(A, \mathbf{1}_2)$ and $\tau(A, B) = \tau(B, A)$.*

*Proof:*
Since $\widetilde{G_n}/\Gamma_n \cong G_n$, we have the isomorphism. We define $\tau : G_n \times G_n \to \Gamma_n$ in the following way

$$\tau(X_1, X_2) = s(X_1)s(X_2)s(X_1X_2)^{-1}$$

where $s$ is any section from $s : G_n \to \widetilde{G_n}$. Any section is fine because we will get an element in $\Gamma_n$. Let $\overline{A}, \overline{B} \in G_n^\tau$, since $A \cdot A^{-1} = \mathbf{1}_2$ and $A \cdot \mathbf{1}_2 = A$ in $\widetilde{G_n}$, by isomorphism, we also have $\overline{A} \cdot \overline{A^{-1}} = \overline{\mathbf{1}_2}$ and $\overline{A} \cdot \overline{\mathbf{1}_2} = \overline{A}$. Therefore $\tau(A, A^{-1}) = \mathbf{1}_2 = \tau(A, \mathbf{1}_2)$.
By the way we have defined $\Gamma_n$, elements in $\Gamma_n$ have unique determinants. Since $det(AB) = det(BA)$ in $\widetilde{G_n}$ and $det(\overline{AB}) = det(\overline{BA})$ in $G_n^\tau$, we must also have $det(\tau(A, B)) = det(\tau(B, A))$ but $\tau$ maps to $\Gamma_n$ so we must have $\tau(A, B) = \tau(B, A)$.

□

As before we define the canonical Ore set denoted again by $\mathcal{T}'$, in $\Lambda(\widetilde{G_n})$ by

$$\mathcal{T}' := \{\lambda \in \Lambda(\widetilde{G_n}) \mid \Lambda(\widetilde{G_n})/\Lambda(\widetilde{G_n})\lambda \text{ is a finitely generated } \mathbb{Z}_p\text{-module}\}$$

We have the following more convenient description of $\Lambda(\widetilde{G_n})_{\mathcal{T}'}$:

**Lemma 2.3** *([10], Lemma 2.1) The set $T = \Lambda(\Gamma_n) - p\Lambda(\Gamma_n)$ is a multiplicatively closed, left and right Ore subset of $\Lambda(\widetilde{G_n})$. The natural injection $\Lambda(\widetilde{G_n})_T \to \Lambda(\widetilde{G_n})_{\mathcal{T}'}$ is an isomorphism.*

Using this lemma we obtain the following result

**Lemma 2.4** *Let $\widehat{\Lambda(\widetilde{G_n})_{\mathcal{T}'}}$ and $\widehat{\Lambda(\Gamma_n)_T}$ denote p-adic completions. Then the natural map*

$$\widehat{\Lambda(\Gamma_n)_T}[G_n]^\tau \xrightarrow{\cong} \widehat{\Lambda(\widetilde{G_n})_{\mathcal{T}'}}$$

*is an isomorphism.*

*Proof:*
By using lemma 2.2 we have the following:

$$\mathbb{Z}_p[[\widetilde{G_n}]] \cong \mathbb{Z}_p[[\Gamma_n]][G_n]^\tau$$

By completing both sides and localizing we get:

$$(\widehat{\Lambda(\Gamma_n)[G_n]^\tau})_{\mathcal{T}'} \cong \widehat{\Lambda(\widetilde{G_n})_{\mathcal{T}'}}$$

We use the lemma 2.3 and the fact the $G_n$ is finite to get the following:

$$\widehat{\Lambda(\Gamma_n)_T}[G_n]^\tau \xrightarrow{\cong} \widehat{\Lambda(\widetilde{G_n})_{\mathcal{T}'}}$$

□

## 2.2 $K$-theory of Iwasawa algebras and localisations

In this section we will first define $K_0$ for rings and categories of certain modules, and then define $K_1$ for rings.

**Definition 2.2** *For any ring $R$, $K_0(R)$ is the Abelian group generated by elements $[P]$, where $P$ is a finitely generated projective $R$-module, with the following relations:*

- *if $P'$ is isomorphic to $P$ as $R$-modules, then $[P] = [P']$*
- *if $P = P' \oplus P''$ then $[P] = [P'] + [P'']$*

**Definition 2.3** *For any ring homomorphism $f : R \to R'$, $K_0(f)$ is the Abelian group generated by elements $[P, g, Q]$, where $P$ and $Q$ are a finitely generated projective $R$-module and $g$ is any isomorphism between $R' \otimes_R P$ and $R' \otimes_R Q$ as $R'$-modules. We have the following relations:*

- *if there exist $h_P : P \xrightarrow{\cong} P'$ and $h_Q : Q \xrightarrow{\cong} Q'$ such that $g' \circ (id_{R'} \otimes h_P) = (id_{R'} \otimes h_Q) \circ g$, then $[P, g, Q] = [P', g', Q']$*
- *if $g = g' \circ g''$ such that $g''$ is any isomorphism between $R' \otimes_R P$ and $R' \otimes_R O$ and $g'$ is any isomorphism between $R' \otimes_R O$ and $R' \otimes_R Q$, then $[P, g, Q] = [P, g'', O] + [O, g', Q]$*
- *if there are three elements $[P, g, Q]$, $[P', g', Q']$ and $[P'', g'', Q'']$ such that we have the following short exact sequences compatible with $g, g'$ and $g''$*

  $$0 \to P' \to P \to P'' \to 0 \quad \text{and} \quad 0 \to Q' \to Q \to Q'' \to 0$$

  *then $[P, g, Q] = [P', g', Q'] + [P'', g'', Q'']$*

We write $K_0(R, R')$ for $K_0(f)$ if $f$ is a canonical injection from $R$ to $R'$.

To define $K_1$, we first need to define $GL(R)$, the **infinite general linear group over** $R$:
We define $GL(R)$ as $\bigcup_{n>0} GL_n(R)$ where we say $GL_n(R) \subset GL_m(R)$ for $n < m$ with the following inclusion:

$$A \in GL_n(R) \implies \begin{pmatrix} A & \mathbf{0} \\ \mathbf{0} & \mathbf{1}_{m-n} \end{pmatrix} \in GL_m(R)$$

where $\mathbf{0}$ are zero matrices and $\mathbf{1}_n$ is the $n$ by $n$ identity matrix.
$[GL(R), GL(R)]$ is called the **commutator subgroup of** $GL(R)$, it is generated by the set $\{ABA^{-1}B^{-1} \mid A, B \in GL(R)\}$.

**Definition 2.4**

$$K_1(R) := \frac{GL(R)}{[GL(R), GL(R)]}$$

*In other words, $K_1(R)$ is the abelianization of the infinite general linear group.*

In our case we have a surjective map $(\Lambda(G))^\times \twoheadrightarrow K_1(\Lambda(G))$ ([4], Theorem 4.4).

Let $I$ be an ideal of $R$, then $GL(R, I)$ is the group of invertible matrices which are congruent to the identity matrix modulo $I$. Now let $E(R, I)$ denote the smallest normal subgroup of $GL(R)$ which contain all elementary matrices[4] which are congruent to the identity modulo $I$. Set $K_1(R, I) := GL(R, I)/E(R, I)$. By Whitehead's lemma ([14], Theorem 1.13) $E(R, I) = [GL(R), GL(R, I)]$, therefore $K_1(R, I)$ is abelian.

[4]Elementary matrices differ from the identity matrix by changing one of the zero entries to some $r \in R$

In the case that we have a finite group $G$, we can use the definition $SK_1(A[G]) := ker(K_1(A[G]) \to K_1(\mathcal{Q}(A)[G]))$ where $A$ is a Dedekind domain with $\mathcal{Q}(A)$ as its field of fractions. In the case that the group $G$ is pro-finite, $G = \varprojlim_U U$, we use the following:

$$SK_1(A[[G]]) := \varprojlim_U SK_1(A[U])$$

**Definition 2.5** *For a Dedekind domain $A$ and a pro-finite group $G$, we have*

$$K_1'(A[[G]]) := K_1(A[[G]])/SK_1(A[[G]])$$

Recall that $\mathcal{G} = GL_2(\mathbb{Z}_p)$. From now on we put $\Lambda = \Lambda(\mathcal{G})$.
Let $\partial$ be defined as the map in the following exact sequence ([19], Theorem 15.5):

$$K_1(\Lambda) \to K_1(\Lambda_{\mathcal{T}'}) \xrightarrow{\partial} K_0(\Lambda, \Lambda_{\mathcal{T}'}) \to K_0(\Lambda) \to K_0(\Lambda_{\mathcal{T}'}) \to 0$$

$$\partial : [f] \mapsto [\Lambda^n, \tilde{f}, \Lambda^n]$$

where $\tilde{f} \in GL_n(\Lambda)$ such that $\tilde{f}$ lifts to $f \in GL(\Lambda)$.
It turns out that $K_0(\Lambda, \Lambda_{\mathcal{T}'})$ maps to 0 in $K_0(\Lambda)$ ([4], Proposition 3.4), thus, by exactness of the sequence, $\partial$ is surjective. As $\mathcal{G}$ has no $p$-torsion, we have the following ([2], Proposition 3.4)

$$K_1(\Lambda_{\mathcal{T}}) \cong K_1(\Lambda_{\mathcal{T}'}) \oplus K_0(\Lambda_{\mathcal{T}'}, \Lambda_{\mathcal{T}})$$

and also that $K_0(\Lambda_{\mathcal{T}'}, \Lambda_{\mathcal{T}}) \cong \mathbb{Z}^r$ for some $r \geq 0$.

## 2.3 Classical Iwasawa theory

In this section we recall formulations of main conjectures using structure theory when $G \cong \mathbb{Z}_p^d$. For the rest of this section we set $G \cong \mathbb{Z}_p^d$. Then $\Lambda(G)$ is non-canonically isomorphic to the power series ring in $d$ variables over $\mathbb{Z}_p$. Fix $d$ elements $\gamma_1, \gamma_2, ..., \gamma_d \in G$ that topologically generate $G$. Then

$$\Lambda(G) \xrightarrow{\cong} \mathbb{Z}_p[[T_1, T_2, ..., T_d]]$$

$$\gamma_i \mapsto T_i + 1$$

The following is the structure theorem for finitely generated modules over $\Lambda(G)$:

**Theorem 2.1** *[1] Let $X$ be a finitely generated $\Lambda(G)$-module, then there is a map*

$$X \to \bigoplus_i \Lambda(G)/(f_i) \oplus \Lambda(G)^r$$

*where the kernel and cokernel are pseudo-null, i.e. they are annihilated by height two ideals of $\Lambda(G)$.*

**Definition 2.6** *A finitely generated $\Lambda(G)$-module $X$ is pseudo-isomorphic to $Y$ if there exists a map*

$$X \to Y$$

*with pseudo-null kernel and cokernel.*

A finitely generated $\Lambda(G)$-module $X$ is called torsion if for every $x \in X$, there exists $f \in \Lambda(G)\backslash\{0\}$ such that $f \cdot x = 0$. In other words, $X$ is a torsion $\Lambda(G)$-module if $\mathcal{Q}(\Lambda(G)) \otimes_{\Lambda(G)} X = 0$, where $\mathcal{Q}(\Lambda(G))$ is the total ring of fractions of $\Lambda(G)$.

In the category of finitely generated torsion $\Lambda(G)$-modules, being pseudo-isomorphic is an

equivalence relation. If $X$ is a finitely generated torsion $\Lambda(G)$-module, then there is a pseudo-isomorphism

$$X \to \bigoplus_i \Lambda(G)/(f_i)$$

for some $f_i$ in $\Lambda(G)$.

**Definition 2.7** *Define the characteristic ideal*

$$char_{\Lambda(G)}(X) = (\prod_i f_i)\Lambda(G)$$

*where the elements $f_i$ are defined as above.*

In classical formulations of main conjectures in Iwasawa theory, one has interesting arithmetic objects $X$ (such as ideal class groups, or Selmer groups) which are torsion or are conjectured to be torsion over $\Lambda(G)$. Thus we can attach an arithmetic invariant $char_{\Lambda(G)}(X)$ to it. The main conjecture may be stated as saying that there is a canonical generator $\mathcal{L}$ of the principal ideal $char_{\Lambda(G)}(X)$ whose "evaluations" at various continuous representations of $G$ are related to $L$-values. We will not make this precise here. Let us only recall what evaluations mean. Let

$$\rho : G \to \overline{\mathbb{Q}_p}^\times$$

be a continuous homomorphism. Then it extends to a map

$$\rho : \Lambda(G) \to \overline{\mathbb{Q}_p}$$

This is classically denoted as $\mu \mapsto \int_G \rho \, d\mu$.
We call it evaluation of $\mu$ at the continuous representation $\rho$.
More information about the classical case can be found in Washington [23].

## 2.4 Reformation using $K$-theory

In [20] and [4] main conjectures are reformulated without using structure theory but by using algebraic $K$-groups, specifically $K_0$ and $K_1$ groups. We continue to assume $G \cong \mathbb{Z}_p^d$. Recall the lower terms of $K$-theory localisation sequence ([19], Theorem 15.5):

$$K_1(\Lambda(G)) \to K_1(\mathcal{Q}(\Lambda(G))) \xrightarrow{\partial} K_0(\Lambda(G), \mathcal{Q}(\Lambda(G))) \to 0$$

A finitely generated torsion $\Lambda(G)$-module gives a class $[X]$ in $K_0(\Lambda(G), \mathcal{Q}(\Lambda(G)))$. Any element $\xi \in K_1(\mathcal{Q}(\Lambda(G)))$ is a called a characteristic element of $X$ if $\partial(\xi) = [X]$. This characteristic element is well-defined up to multiplication by an element in $\Lambda(G)^\times$. By ([20], Remark 6.2), we know that this definition of characteristic element is a generalized version of the one stated above.

Now let $G$ be any $p$-adic Lie group. The localisation sequence for $\Lambda(G)$ and $\mathcal{Q}(\Lambda(G))$ exists and one may use it to formulate main conjectures. For many technical reasons (as explained in [20]) it is better to restrict to $G$ having a closed normal subgroup $H$ such that $G/H = \Gamma \cong \mathbb{Z}_p$ and working with a smaller localisations $\Lambda(G)_{\mathcal{T}'}$ or $\Lambda(G)_{\mathcal{T}}$. Here

$$\mathcal{T}' := \{\lambda \in \Lambda(G) \mid \Lambda(G)/\Lambda(G)\lambda \text{ is a finitely generated } \Lambda(H)\text{- module}\}$$

and $\mathcal{T} := \bigcup_{i \geq 0} p^i \mathcal{T}'$.
As proven in [4], $\mathcal{T}'$ and $\mathcal{T}$ are multiplicatively closed subset of $\Lambda(G)$, they do not contain zero divisors and they satisfy the Ore condition (left and right). Furthermore, we have localisation sequences:

$$K_1(\Lambda(G)) \to K_1(\Lambda(G)_{\mathcal{T}'}) \xrightarrow{\partial} K_0(\Lambda(G), \Lambda(G)_{\mathcal{T}'}) \to 1$$

$$K_1(\Lambda(G)) \to K_1(\Lambda(G)_{\mathcal{T}}) \xrightarrow{\partial} K_0(\Lambda(G), \Lambda(G)_{\mathcal{T}}) \to 1$$

Let $T \in \{\mathcal{T}', \mathcal{T}\}$. If $X$ is a finitely generated $\Lambda(G)$-module which is $T$-torsion[5] then $X$ gives a class $[X]$ in $K_0(\Lambda(G), \Lambda(G)_T)$. Any element $\xi$ in $K_1(\Lambda(G)_T)$ such that $\partial(\xi) = [X]$ is called a characteristic element of $X$. In this setting the main conjecture simply gives a characteristic element whose "evaluations" are related to $L$-values. Let us explain evaluations in this setting. Let

$$\rho : G \to GL_n(\mathcal{O})$$

be a continuous homomorphism, for the ring of integers $\mathcal{O}$ in a finite extension $L$ of $\mathbb{Q}_p$.
Then this extends to a map from $K_1(\Lambda(G)_{\mathcal{T}'})$ to $L \bigcup \{\infty\}$; we will state this map after we define the augmentation map:

$$\varphi : \Lambda_{\mathcal{O}}(\Gamma)_{\mathfrak{p}} \to L$$
$$\varphi : \sum x_g g \mapsto \sum x_g$$

where $\Lambda_{\mathcal{O}}(\Gamma) = \mathcal{O}[[\Gamma]]$ and $\mathfrak{p}$ is the kernel of the augmentation map from $\Lambda_{\mathcal{O}}(\Gamma)$ to $\mathcal{O}$. The map $\rho$ extends to the following map:

$$\xi(\rho) := \begin{cases} \varphi(\Phi_\rho(\xi)) & \text{if } \Phi_\rho(\xi) \in \Lambda_{\mathcal{O}}(\Gamma)_{\mathfrak{p}} \\ \infty & \text{if } \Phi_\rho(\xi) \notin \Lambda_{\mathcal{O}}(\Gamma)_{\mathfrak{p}} \end{cases}$$

We will define $\Phi_\rho$ now:
Let $\mathcal{Q}(\Lambda_{\mathcal{O}}(\Gamma))$ be the field of fractions of $\Lambda_{\mathcal{O}}(\Gamma)$, then by ([4], Lemma 3.3), we have a ring homomorphism $\Lambda(G)_{\mathcal{T}'} \to M_n(\mathcal{Q}(\Lambda_{\mathcal{O}}(\Gamma)))$ defined by $\sum x_g g \mapsto \sum x_g(\rho(g) \otimes \overline{g})$ where $\overline{g}$ is the image of $g \in G$ under the projection of $G \to \Gamma$. This homomorphism induces the following homomorphism:

$$\Phi_\rho : K_1(\Lambda(G)_{\mathcal{T}'}) \to K_1(M_n(\mathcal{Q}(\Lambda_{\mathcal{O}}(\Gamma)))) = (\mathcal{Q}(\Lambda_{\mathcal{O}}(\Gamma)))^\times$$

Following the classical notation we may denote the map as

$$\mu \mapsto \int_G \rho \, d\mu = \xi(\rho)$$

**Remark:** Here we remark that if $G \cong \mathbb{Z}_p$ then $\Lambda(G)_{\mathcal{T}'} = \mathcal{Q}(\Lambda(G))$. Furthermore any finitely generated $\Lambda(G)$-module has a finite projective resolution.

Instead of $X$ as above, we may even take a perfect complex $C^\bullet$ of $\Lambda(G)$-modules whose cohomologies are $T$-torsion i.e. $\Lambda(G)_T \bigotimes^L_{\Lambda(G)} C^\bullet$ is acyclic.

## 2.5 The $GL_2$ main conjecture for elliptic curves

In this chapter we will state the $GL_2$ main conjecture for elliptic curves, but first we need to define many objects we will need:

$$K_n := \mathbb{Q}(E[p^n]), \quad K_\infty := \bigcup_{n \geq 1} K_n, \quad \mathcal{G} = Gal(K_\infty/\mathbb{Q})$$
$$\Lambda := \Lambda(\mathcal{G}) = \mathbb{Z}_p[[\mathcal{G}]] := \varprojlim_n \mathbb{Z}_p[Gal(K_n/\mathbb{Q})]$$

[5] A module $X$ is $T$-torsion if $\forall x \in X$, there exists $t \in T$ such that $t \cdot x = 0$.

### 2.5.1 The Selmer group of $E$

In this chapter we want to define $Sel(E/K_\infty)$, the $p$-Selmer group of $E$ over $K_\infty$. Let $L$ be an algebraic extension of $\mathbb{Q}$, $L_\nu$ is the completion of $L$ at a place $\nu$ and $\overline{L_\nu}$ is an algebraic closure of $L_\nu$. Also, $E(\overline{L_\nu})$ are the $\overline{L_\nu}$-rational points and $E_{p^\infty} = \bigcup_{n>0} E[p^n]$. Finally, $H^1(L, E_{p^\infty}) := H^1(G_L, E_{p^\infty})$ is the 1st Galois cohomology group such that $G_L$ is the absolute Galois group of $L$; the action of $G_L$ on $E_{p^\infty}$ is the action induced by the natural action of $G_L$ on $E_{tors} \cong (\mathbb{Q}/\mathbb{Z})^2$, where $E_{tors}$ is the torsion subgroup of $E(\overline{\mathbb{Q}})$.

$$Sel(E/L) := ker((H^1(L, E_{p^\infty}) \to \prod_\nu H^1(L_\nu, E(\overline{L_\nu})))$$

where the product runs over all places of $L$. In our case, $L = K_\infty$ is an infinite extension of $\mathbb{Q}$ so we define the completion to be $L_\nu = \bigcup (L')_\nu$ where we union over the set of all finite extensions, $L'$ over $\mathbb{Q}$, which are contained in $L$.

The Selmer group and the Tate-Shafarevich group[6], $Sha$, can tell us about the corresponding elliptic curve as one can see by the following exact sequence:

$$0 \to E(L) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to Sel(E/L) \to Sha(E/L)(p) \to 0$$

where $Sha(E/L)(p)$ denotes the $p$-primary part of $Sha(E/L)$.

$$X := X(E/K_\infty) = Sel(E/K_\infty)^\vee, \text{ this is the Pontryagin dual of the Selmer group}$$

i.e. $X(E/K_\infty) = Hom(Sel(E/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$. It turns out that $X(E/K_\infty)$ is finitely generated over $\Lambda$ ([5], Theorem 2.9).

### 2.5.2 $p$-adic $L$-function of $E$, $\mathcal{L}_E$

The $p$-adic $L$-function of $E$, $\mathcal{L}_E$, is a conjectural element of $K_1(\Lambda_{\mathcal{T}})$ and we expect it to be a characteristic element of $X$. Before defining $\mathcal{L}_E$, we will define the $L$-function of $E$, $L(E, \rho, s)$, where $\rho$ is an Artin representation[7]of $\mathcal{G}$. Let $A(\mathcal{G})$ be the set of Artin representations of $\mathcal{G}$ and let $l$ and $q$ be two distinct prime numbers.

Let $I_l$ be the inertia group of $G_{\mathbb{Q}_l}$, the subgroup of $G_{\mathbb{Q}_l}$ which fixes $\mathbb{Z}_l/l\mathbb{Z}_l$, and $Frob_l$ be the Frobenius automorphism of $l$ in $G_{\mathbb{Q}_l}/I_l = Gal(\overline{\mathbb{Q}_l}/\mathbb{Q}_l)/I_l$. Also let $K_\rho$ be a finite extension of $\mathbb{Q}$ such that we have the vector space associated to $\rho$ defined over $K_\rho$, and call this vector space $V_\rho$. Also let $H^1_q(E) := Hom(T_q(E) \otimes_{\mathbb{Z}_q} \mathbb{Q}_q, \mathbb{Q}_q)$ such that $T_q(E) := \varprojlim_n E[q^n]$ is the **$q$-adic Tate module** of $E$. Finally, let $\lambda$ be a prime of $K_\rho$ above $q$, then $P_l(E, \rho, T) := det(\mathbf{1} - Frob_l^{-1}T\,;\, (H^1_q(E) \otimes_{\mathbb{Q}_q} (V_\rho \otimes_K K_{\rho,\lambda}))^{I_l})$ (we have used the following notation[8]; $det(\mathbf{1} - gT\,;\, V_\rho) = det(\mathbf{1} - \rho(g)T)$ where $V_\rho$ is the associated vector space to the representation $\rho$). Then the $L$-function of $E$ is defined by the following Euler product:

$$L(E, \rho, s) = \prod_l P_l(E, \rho, l^{-s})^{-1}$$

where the product is over all primes $l$.

---

[6] Tate-Shafarevich group of $E/L$:

$$Sha(E/L) := ker((H^1(L, E(\overline{L})) \to \prod_\nu H^1(L_\nu, E(\overline{L_\nu}))))$$

[7] An Artin representation $\rho : \mathcal{G} \to GL_n(\mathbb{Z}_p)$ is a continuous representation such that $ker(\rho)$ is open.

[8] The reason we use the representation associated to a vector space which is fixed by $I_l$, is because $Frob_l$ lives in $Gal(\mathbb{Q}_l^{unram}/\mathbb{Q}_l)$ where $\mathbb{Q}_l^{unram}$ is the maximal unramified extension over $\mathbb{Q}_l$.

Let $R = \{p\} \bigcup \{l \text{ prime} \mid ord_l(j_E) < 0\}$ where $j_E$ is the $j$-**invariant**[9]of $E$. We define $L_R(E, \rho, s)$ to be the $L$-function with Euler factors removed of the primes in $L$, i.e:

$$L_R(E, \rho, s) = \prod_{l \notin R} P_l(E, \rho, l^{-s})^{-1}$$

Now we are ready to define $\mathcal{L}_E$:

**Conjecture 2.1** *([2], Conjecture 7.3) Let $M$ be the motive $h^1(E)(1)$. Assume that $p \geq 5$ and that $E$ has good ordinary reduction at $p$. Then $\exists \mathcal{L}_E \in K_1(\Lambda_{\mathcal{T}})$ such that for all Artin representations of $\mathcal{G}$, the value at $T = 0$ of $T^{-r(M)(\rho)}\Phi_\rho(\mathcal{L}_E)$ is equal to*

$$(-1)^{r(M)(\rho)} \frac{L_R(E, \rho^*, 1)}{\Omega_\infty(M(\rho^*))R_\infty(M(\rho^*))} \cdot \Omega_p(M(\rho^*))R_p(M(\rho^*)) \cdot \frac{P_{L,p}(\hat{W}^*_\rho(1), 1)}{P_{L,p}(\hat{W}_\rho, 1)}$$

For the purposes of this thesis, it is not important to define all of the notation in the above conjecture, but it is all defined in Section 7 of [2].

### 2.5.3 The main conjecture

We can now state the Main Conjecture:

**Conjecture 2.2** *([4], Conjecture 5.8) Assume that $p \geq 5$, that $E$ has good ordinary reduction at $p$, and that $X := X(E/K_\infty)$ is a finitely generated torsion $\Lambda(G)$-module. Granted Conjecture 2.1, the $p$-adic $L$-function $\mathcal{L}_E \in K_1(\Lambda_{\mathcal{T}})$ is a characteristic element of $X$.*

The important aspect to notice about Conjecture 2.2, is that we have an element that is related to $L$-values when acted on by different Artin characters, and it is also a characteristic element of $X$. If the main conjecture were proved, we would have the following:

**Corollary 2.1** *([4], Corollary 5.9) Assume Conjecture 2.2. For any Artin representation of $\mathcal{G}$, $\rho \in A(\mathcal{G})$, let $\hat{\rho}(g) = \rho(g^{-1})^T$ where the $T$ stands for transpose. $\forall \rho \in A(\mathcal{G})$, such that $\rho$ lands in $GL_d(\mathbb{Z}_p)$, $L(E, \hat{\rho}, 1) \neq 0 \iff \prod_{i \geq 0} \#H_i(\mathcal{G}, tw_\rho(X))^{(-1)^i}$ is finite where $tw_\rho(X) = X \otimes_{\mathbb{Z}_p} \mathbb{Z}_p^d$ such that we endow $tw_\rho(X)$ with the diagonal action. In this case, by ([4], Theorem 3.6), we have $\prod_{i \geq 0} \#H_i(\mathcal{G}, tw_\rho(X))^{(-1)^i} = |\mathcal{L}_E(\rho)|_p^d$.*

## 2.6 The goal of this paper

### 2.6.1 The strategy of Kato

It is important for us to calculate $K_1(\Lambda)$. As we mentioned at the end of section 2.2, we have $K_1(\Lambda_{\mathcal{T}}) \cong K_1(\Lambda_{\mathcal{T}'}) \oplus \mathbb{Z}^r$ for some $r \geq 0$. Thus we only study $K_1(\Lambda_{\mathcal{T}'})$. Our methods use logarithms and thus we need $p$-adically completed rings, hence we study $K_1\left(\widehat{\Lambda}_{\mathcal{T}'}\right)$. As explained earlier, we study $K_1(\Lambda)$ and $K_1\left(\widehat{\Lambda}_{\mathcal{T}'}\right)$ by studying $K_1(\mathbb{Z}_p[G_n])$ and $K_1\left(\widehat{\Lambda(\widetilde{G_n})}_{\mathcal{T}'}\right)$. To do this we will imitate the method used by Kakde in the proof of the non-commutative main conjecture for totally real fields.

Using the strategy of Burns and Kato, Kakde [11] proved the non-commutative main conjecture for totally real fields under the $\mu = 0$ condition ([11], Definition 2.8). In this proof, Kakde

[9] $j$-invariant: Let $E$ be $y^2 = x^3 + bx + c$, then the $j$-invariant of $E$ is $j_E := 1728\frac{b^3}{b^3 - 27c^2}$. $ord_l(a)$ is the integer such that $l^{ord_l(a)} || a$.

constructed the following commutative diagram to obtain a description of $K_1'$ groups ([11], Proof of Theorem 5.16):

$$\begin{array}{ccccccccccc} 1 & \to & ker(Log) & \to & K_1'(\Lambda(G)) & \xrightarrow{Log} & \mathcal{O}[[Conj(G)]] & \to & coker(Log) & \to & 1 \\ & & =\downarrow & & \theta\downarrow & & \psi\downarrow\cong & & =\downarrow & & \\ 1 & \to & ker(\mathcal{L}) & \to & \Theta & \xrightarrow{\mathcal{L}} & \Psi & \to & coker(\mathcal{L}) & \to & 1 \end{array}$$

Explaining the details of this diagram[10]is not necessary at this point, but it will be explained in section 2.6.2.
The aim of this paper is to build on that work, and construct a similar diagram in the elliptic curve case to obtain descriptions for $K_1\left(\mathbb{Z}_p[G_n]\right)$ and $K_1\left(\widehat{\Lambda(\widetilde{G_n})_{\mathcal{T}'}}\right)$ (see Section 2.6.2 for details).

### 2.6.2 Our strategy

Recall that $\mathcal{G} = GL_2(\mathbb{Z}_p)$. In this section $G$ is a finite group.

We will start this section by defining two important maps; *Log*, the **integral logarithm** ([14], Definition 6.1), and the map $\psi$. We will start with *Log*, which depends on the prime $p$ from the domain, $\mathbb{Z}_p$:

**Definition 2.8** *([14], Definition 6.1) Let $\varphi$ be the endomorphism of $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G]/[\mathbb{Z}_p[G], \mathbb{Z}_p[G]]$ induced by the map $\sum x_g g \mapsto \sum x_g g^p$. The integral logarithm is a map which is defined as follows:*

$$Log : K_1(\mathbb{Z}_p[G]) \to \mathbb{Z}_p[G]/[\mathbb{Z}_p[G], \mathbb{Z}_p[G]]$$

$$Log : x \mapsto log(x) - \frac{1}{p}\varphi(log(x))$$

*where $[\mathbb{Z}_p[G], \mathbb{Z}_p[G]]$ denotes the additive group generated by elements $[a_1, a_2]$ such that $a_1, a_2 \in \mathbb{Z}_p[G]$.*

[10]One thing that should be noted is that the $G$ here is the Galois group defined in a similar way to our $\mathcal{G}$ but for totally real fields instead of elliptic curves.

The integral logarithm lands in $\mathbb{Z}_p[G]/[\mathbb{Z}_p[G],\mathbb{Z}_p[G]]$ by ([14], Theorem 6.2):
*Idea of the Proof:*
For $x$ in the Jacobson radical of $\mathbb{Z}_p[G]$ one has:

$$Log(1-x) \equiv -\sum_{k=1}^{\infty} \frac{1}{pk}(x^{pk} - \varphi(x^k)) \ (mod\ \mathbb{Z}_p[G]/[\mathbb{Z}_p[G],\mathbb{Z}_p[G]])$$

So one needs to show that $pk|(x^{pk} - \varphi(x^k))$, but in $\mathbb{Z}_p$, only $p$ is non-invertible, so we can set $k = p^{n-1}$ where $n$ is a positive integer. So we just need to show $p^n|(x^{p^n} - \varphi(x^{p^{n-1}}))$. To show this, one expands $x$ as $\sum a_g g$, then one looks at the expansion of $x^{p^n}$ and then one finds that this expansion is made up of terms in the form $p^{n-t}a_g^{p^t}g^{p^t}$ for some $t$, $0 \leq t \leq n$. By definition of $\varphi$, we know $p|(a_g^p - \varphi(a_g))$, but when comparing $x^{p^n}$ with $\varphi(x^{p^{n-1}}))$ we then find that $p^{n-t}a_g^{p^t}g^{p^t} \equiv p^{n-t}\varphi(a_g^{p^{t-1}})g^{p^t}\ (mod\ p^n)$, therefore $p^t|(a_g^{p^t} - \varphi(a_g^{p^{t-1}}))$, so we have the desired result.

Let $Conj(G)$ be the set of all conjugacy classes $[A]_G$ of elements $A \in G$.

**Proposition 2.1** *([17], Lemma 2.1) Let $\mathbb{Z}_p[Conj(G)]$ denote the free $\mathbb{Z}_p$-module over the basis $Conj(G)$. Then we have isomorphism:*

$$\mathbb{Z}_p[G]/[\mathbb{Z}_p[G],\mathbb{Z}_p[G]] \cong \mathbb{Z}_p[Conj(G)]$$

*as $\mathbb{Z}_p$-modules.*

Before defining $\psi$, there is one last important property of *Log* we should state. Let $\hat{G} = \{g \in G | g \text{ has order prime to } p\}$ and let $\beta_n$ be the automorphism of $H_n(G,\mathbb{Z}_p(\hat{G}))$ induced by the map $\sum x_g g \mapsto \sum x_g g^p$. If we look at *Log* as a map on the pro-$p$ part of $K_1(\mathbb{Z}_p[G])$, then by ([14], Theorem 12.9(iii)), the kernel of *Log* is $SK_1(\mathbb{Z}_p[G]) \oplus H_1(G,\mathbb{Z}_p(\hat{G}))^{\beta_1} \oplus H_0(G,(\mathbb{Z}_p/2\mathbb{Z}_p)(\hat{G}))^{\beta_0}$ and the cokernel of *Log* is $SK_1(\mathbb{Z}_p[G]) \oplus H_1(G,\mathbb{Z}_p(\hat{G}))_{\beta_1} \oplus H_0(G,(\mathbb{Z}_p/2\mathbb{Z}_p)(\hat{G}))_{\beta_0}$ where $H_n(G,\mathbb{Z}_p(\hat{G}))^{\beta_n} = ker(1-\beta_n)$ and $H_n(G,\mathbb{Z}_p(\hat{G}))_{\beta_n} = coker(1-\beta_n)$. Since we are taking $p > 2$, we have that $H_0(G,(\mathbb{Z}_p/2\mathbb{Z}_p)(\hat{G}))_{\beta_0}$ is trivial.

**Definition 2.9** *Let $U$ be a subgroup of $\mathcal{G}$ and let $[A]_U$ indicate the conjugacy class of $A$ as an element of $U$. Let $Tr_{\mathcal{G}/U}$ be the map:*

$$\begin{array}{ccc} \mathbb{Z}_p[Conj(\mathcal{G})] & \to & \mathbb{Z}_p[Conj(U)] \\ [A]_{\mathcal{G}} & \mapsto & \sum_{\substack{X \in U\backslash\mathcal{G} \\ X^{-1}AX \in U}} [X^{-1}AX]_U \end{array}$$

*and let $proj_U$ be the natural projection from $\mathbb{Z}_p[Conj(U)]$ to $\mathbb{Z}_p[Conj(U^{ab})] = \mathbb{Z}_p[U^{ab}]$, then:*

$$\begin{array}{ccc} \psi : \mathbb{Z}_p[Conj(\mathcal{G})] & \to & \prod_{U\in\mathcal{F}} \mathbb{Z}_p[U^{ab}] \\ \psi : [A]_{\mathcal{G}} & \mapsto & \prod_{U\in\mathcal{F}} proj_U \circ Tr_{\mathcal{G}/U}([A]_{\mathcal{G}}) \end{array}$$

As mentioned in the above section, we want to imitate the commutative diagram that was mentioned in that section:

$$\begin{array}{ccccccccc} ker(Log) & \to & K_1(\mathbb{Z}_p[[\mathcal{G}]]) & \xrightarrow{Log} & \mathbb{Z}_p[[Conj(\mathcal{G})]] & \to & coker(Log) & & \\ & & \downarrow \theta & & \downarrow \psi & & & & (1) \\ ker(\mathcal{L}) & \dashrightarrow & \Theta & \xrightarrow{\mathcal{L}} & \Psi & \dashrightarrow & coker(\mathcal{L}) & & \end{array}$$

Here $\Psi \subset \prod_{U\in\mathcal{F}} \Lambda(U^{ab}) \subset \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \prod_{U\in\mathcal{F}} \Lambda(U^{ab})$ is the image[11]of $\psi$ and $\Theta \subset \prod_{U\in\mathcal{F}} \Lambda(U^{ab})^\times$ is a group that contains the image of $\theta$. The bottom arrows are dotted to represent that they were conjectural before they were constructed in this paper.

[11]The image of $\psi$ lies in $\prod_{U\in\mathcal{F}} \mathbb{Z}_p[U^{ab}]$ but we expect the image of $\prod_{U\in\mathcal{F}} \Lambda(U^{ab})^\times$, under the map $\mathcal{L}$, to lie outside of $\prod_{U\in\mathcal{F}} \mathbb{Z}_p[U^{ab}]$. This is why we are also interested in looking at $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \prod_{U\in\mathcal{F}} \mathbb{Z}_p[U^{ab}]$

To construct the map $\mathcal{L}$, first we find $\mathbb{Z}_p[[Conj(\mathcal{G}))]]$. Secondly, we want to show $\psi$ is injective for our choice of $\mathcal{F}$ and then describe its image, $\Psi$. A description of $\Psi$ will help us define $\mathcal{L}$ by using the following diagram ([14], Proof of Theorem 6.8):

$$\begin{array}{ccccc} K_1(\mathbb{Z}_p[[\mathcal{G}]]) & \xrightarrow{log} & \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[Conj(\mathcal{G})]] & \xrightarrow{1-\frac{\varphi}{p}} & \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[Conj(\mathcal{G})]] \\ \downarrow \theta & \circlearrowright & \downarrow \psi & & \downarrow \psi \\ \prod_{U\in\mathcal{F}} \Lambda(U^{ab})^\times & \xrightarrow{log} & \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \prod_{U\in\mathcal{F}} \mathbb{Z}_p[[U^{ab}]] & \dashrightarrow & \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \prod_{U\in\mathcal{F}} \mathbb{Z}_p[[U^{ab}]] \end{array}$$

Notice that the bottom maps combine to give us $\mathcal{L}$. The first square is commutative so we can concentrate on the second square. Since we will have a description for $\mathbb{Z}_p[[Conj(\mathcal{G})]]$ and we will understand $\psi$ much better at this point, for any element $x \in \mathbb{Z}_p[[Conj(\mathcal{G})]]$, we can compute $\psi(x)$ and $\psi((1-\frac{\varphi}{p})(x)$ and compare these two elements to construct a map $\mathcal{L}$. When we have a map $\mathcal{L}$, we can obtain a description of $\Theta$ by calculating a possible pre-image of $\Psi$ under the map $\mathcal{L}$.
If we could also prove that $coker(Log)$ injects into $coker(\mathcal{L})$ and that $ker(Log)$ surjects onto $ker(\mathcal{L})$, then we would know that $\theta$ surjects onto $\Theta$, but unfortunately we cannot do that in this paper.

Let $G_n = GL_2(\mathbb{Z}/p^n\mathbb{Z})$, by a result of Kakde ([11], Lemma 4.1)[12], we can see that $K_1(\mathbb{Z}_p[[\mathcal{G}]]) \cong \varprojlim_n K_1(\mathbb{Z}_p[G_n])$ where the inverse limit is defined by projection. As a result we can reduce diagram (1) and look at the following diagram:

$$\begin{array}{ccccccccc} ker(Log) & \to & K_1(\mathbb{Z}_p[G_n]) & \xrightarrow{Log} & \mathbb{Z}_p[Conj(G_n)] & \to & coker(Log) \\ & & \downarrow \theta & & \downarrow \psi & & \\ ker(\mathcal{L}) & \dashrightarrow & \prod_{U\in\mathcal{F}_n} \Lambda(U^{ab})^\times & \xrightarrow{\mathcal{L}} & \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \prod_{U\in\mathcal{F}_n} \mathbb{Z}_p[U^{ab}] & \dashrightarrow & coker(\mathcal{L}) \end{array}$$

where $\mathcal{F}_n$ is a subgroup of $\mathcal{F}$ such that $\mathcal{F} = \cup_{m\geq 1}\mathcal{F}_m$.

So we can prove that $\psi$ is injective by proving the restrictions of $\psi$ to $G_n$ is injective for all $n$:

$$\psi_n : \mathbb{Z}_p[Conj(G_n)] \longrightarrow \prod_{U\in\mathcal{F}_n} \mathbb{Z}_p[U^{ab}]$$

In this paper we calculate the image of $\psi_n$ for general $n$ and we call this image $\Psi_{n,\mathbb{Z}_p}$. We also construct the map $\mathcal{L}$ and we construct a subgroup of $\prod_{U\in\mathcal{F}} \Lambda(U^{ab})^\times$ which, under the map $\mathcal{L}$, contains $\Psi_{n,\mathbb{Z}_p}$; we call this group $\Theta_{n,\mathbb{Z}_p}$ and it contains the image of $K_1(\mathbb{Z}_p[G_n])$ under the map $\theta_n$. We also verify a similar result for $K_1\left(\widehat{\Lambda(\widehat{G_n})_{\mathcal{T}'}}\right)$. To carry on the work in this paper, the next thing to do would be to calculate the kernel and cokernel of both $Log$ and $\mathcal{L}$. The work in this paper is all done for a particular choice of $\mathcal{F}_n$, which we stated in the next chapter.

[12] This result is a based on a result of Fukaya and Kato ([7], Proposition 1.5.1)

# Chapter 3

# Choosing $\mathcal{F}_n$, a suitable set of subgroups of $G_n$

In this chapter, we want to choose a set $\mathcal{F}_n$ of subgroups of $G_n$ such that the kernel of $\theta$ would be $SK_1(\mathbb{Z}_p[G_n])$. We can achieve this result by using the set of all open subgroups [11] but then we make it much harder to describe the image of $\psi_n$ (Definition 2.9), and as a consequence, it becomes harder to prove the main conjecture via the above strategy. Thus we aim to pick a $\mathcal{F}_n$ which is not too large yet it has the desired kernel.

## 3.1 Computing the $p$-part of the torsion subgroup of $K_1(\mathbb{Z}_p[G_n])$

To help us choose $\mathcal{F}_n$ which gives us the kernel $SK_1(\mathbb{Z}_p[G_n])$, we look at the $p$-part of the torsion subgroup of $K_1(\mathbb{Z}_p[G_n])$. We do that in this chapter by using the following theorem:

**Theorem 3.1** *([14], Theorem 12.5) Fix a prime p, let $F$ be any finite extension of $\mathbb{Q}_p$, and let $R \subset F$ be the ring of integers. For any finite group $G$, let $g_1$,...,$g_k$ be $F$-conjugacy class[1] representatives for elements in $G$ of order prime to $p$, and set*

$$N_i = N_G^F(g_i) = \{x \in G : xg_ix^{-1} = g_i^a,\ \text{some } a \in Gal(F\zeta_{n_i}/F)\}\ (n_i = |g_i|)$$

*and $Z_i$ to be the centralizer group of $g_i$ as an element of $G$. Then*

1. $SK_1(R[G]) \cong \bigoplus_{i=1}^k H_0(N_i/Z_i; H_2(Z_i)/H_2^{ab}(Z_i))_{(p)}$
2. $tors(K_1'(R[G]))_{(p)} \cong [(\mu_F)_p]^k \oplus \bigoplus_{i=1}^k H^0(N_i/Z_i; Z_i^{ab})_{(p)}$

$H_0$ and $H^0$ are the zeroth homology and cohomology[2] respectively. $H_2(Z_i) = H_2(Z_i, \mathbb{Z})$ and $H_2^{ab}(Z_i)$ will be defined later. In our case $[(\mu_F)_p]$ is trivial because we are taking $F = \mathbb{Q}_p$. When defining $\mathcal{F}_n$ it is important to include the subgroups $U$ such that $\prod_U \mathbb{Z}_p[U]$ contains $tors(K_1'(R[G]))_{(p)}$. This is because, by definition of $Log$, these subgroups lie in the kernel of $Log$ and we need $ker(Log)$ to surject onto $ker(\mathcal{L})$.

Here we will just state the full list of the representatives of conjugacy classes of $G_n$ (see the next section for the proof that this list is the full list):

[1] Let $g$ and $h$ be a group elements of order $n$ in $G$. Since $Gal(F\zeta_n/F)$ is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$, Oliver writes $g^a$ to denote the action of $a$ on $g$ for $a \in Gal(F\zeta_n/F)$. We say $g$ and $h$ are $F$-conjugate if $xhx^{-1} = g^a$.

| $A_I$ | $A_B$ | $A_T$ | $A_K$ | $A_{RT,i}$ | $A_{RK,i}$ |
|---|---|---|---|---|---|
| $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ | $\begin{pmatrix} x & 0 \\ 1 & x \end{pmatrix}$ | $\begin{pmatrix} w & y^2 \\ 1 & w \end{pmatrix}$ | $\begin{pmatrix} z & \epsilon y^2 \\ 1 & z \end{pmatrix}$ | $\begin{pmatrix} x & p^i\alpha^2 \\ 1 & x \end{pmatrix}$ | $\begin{pmatrix} x & p^i\epsilon\alpha^2 \\ 1 & x \end{pmatrix}$ |

| $A_{RB,j}$ | $A_{RBI,j,i}$ | $A_{RBJ,j,i}$ | $A_{RI,j}$ | $A_{RJ,j}$ |
|---|---|---|---|---|
| $\begin{pmatrix} x & 0 \\ p^j & x \end{pmatrix}$ | $\begin{pmatrix} x & p^i\alpha^2 \\ p^j & x \end{pmatrix}$ | $\begin{pmatrix} x & p^i\epsilon\alpha^2 \\ p^j & x \end{pmatrix}$ | $\begin{pmatrix} x & p^j\beta^2 \\ p^j & x \end{pmatrix}$ | $\begin{pmatrix} x & p^j\epsilon\beta^2 \\ p^j & x \end{pmatrix}$ |

$$i, j = 1, 2, ..., n-1 \text{ s.t } j < i,\ x, y \in (\mathbb{Z}/p^n\mathbb{Z})^\times \text{ and } w, z \in \mathbb{Z}/p^n\mathbb{Z} \text{ s.t } y \not\equiv \pm w\ (mod\ p)$$

$$\alpha \in (\mathbb{Z}/p^{n-i}\mathbb{Z})^\times \text{ and } \beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times$$

The letter on the top represents the matrix under that letter.
In section 3.3 we calculate how many elements in $G_n$ have order prime to $p$ and what form these matrices are in; there are only $p(p-1)$ distinct conjugacy classes with matrices of order prime to $p$, and they all have a representation matrix in the form $A_I$, $A_T$ or $A_K$ (defined in the table below). The centralizer groups for these matrices are as follows:

| Representatives | Centralizers | no. of prime to $p$ classes |
|---|---|---|
| $A_I := \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ | $GL_2(\mathbb{Z}/p^n\mathbb{Z})$ | $p-1$ |
| $A_T := \begin{pmatrix} w & y^2 \\ 1 & w \end{pmatrix}$ | $\left\{ \begin{pmatrix} a & by^2 \\ b & a \end{pmatrix} : \begin{matrix} a \in \mathbb{Z}/p^n\mathbb{Z} \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{matrix} : p \not\mid (a^2 - b^2y^2) \right\}$ | $\frac{(p-1)(p-2)}{2}$ |
| $A_K := \begin{pmatrix} z & \epsilon y^2 \\ 1 & z \end{pmatrix}$ | $\left\{ \begin{pmatrix} a & b\epsilon y^2 \\ b & a \end{pmatrix} : \begin{matrix} a \in \mathbb{Z}/p^n\mathbb{Z} \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{matrix} : p \not\mid (a^2 - b^2\epsilon y^2) \right\}$ | $\frac{p(p-1)}{2}$ |

We will refer to these centralizer groups as $Z_I$, $Z_T$, and $Z_K$ respectively. We will also denote the normalizer groups in a similar way, i.e. $N_I$, $N_T$, and $N_K$ respectively. $Z_T$ and $Z_K$ are abelian[3], therefore we have $H_2^{ab}(Z_T) = H_2(Z_T)$ and $H_2^{ab}(Z_K) = H_2(Z_K)$ (this will become clear later when we define the second homology). Since the order of elements in the form $A_I$ and $A_T$ are either 1 or $p-1$ (see section 3.3) and $\zeta_{p-1} \in \mathbb{Q}_p$, we have $N_I = Z_I$ and $N_T = Z_T$. So we only need to work out $N_K$:

$$\tilde{A_K} := \begin{pmatrix} z & \epsilon y \\ y & z \end{pmatrix} = \begin{pmatrix} 0 & \epsilon y \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} z & \epsilon y^2 \\ 1 & z \end{pmatrix} \begin{pmatrix} 0 & \epsilon y \\ 1 & 0 \end{pmatrix}$$

Therefore we have $[A_K] = \left[\tilde{A_K}\right]$ and we have $\tilde{A_K} \in K_n := \left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} : \begin{matrix} a, b \in \mathbb{Z}/p^n\mathbb{Z} \\ \text{s.t. } p \not\mid (a^2 - \epsilon b^2) \end{matrix} \right\}$

Since $K_n$ is a group, any power of the matrix $\tilde{A_K}$ will also lie in $K_n$. By definition, if $X \in N_K$ then we must have $X^{-1}A_KX = (A_K)^m$ for some $m$, but any conjugate of $\tilde{A_K}$ lies in $K_n$ in only two cases:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} z & \epsilon y \\ y & z \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} z & \epsilon y \\ y & z \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} z & \epsilon y \\ y & z \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} z & -\epsilon y \\ -y & z \end{pmatrix}$$

[2] $H_0(G;M) = M_G = M/\langle gm - m | g \in G, m \in M \rangle$ and $H^0(G;M) = M^G = \{m \in M | gm - m = 0\ \forall g \in G\}$.

[3] Observe the following:

$$\begin{pmatrix} a & bu \\ b & a \end{pmatrix}^{-1} \begin{pmatrix} c & du \\ d & c \end{pmatrix} \begin{pmatrix} a & bu \\ b & a \end{pmatrix} = \begin{pmatrix} c & du \\ d & c \end{pmatrix}$$

where $a, b, c, d \in \mathbb{Z}/p^n\mathbb{Z}$ such that $p \not\mid a^2 - b^2u$ and $p \not\mid c^2 - d^2u$. Notice that $u$ can be replaced with $y^2$ or $\epsilon y^2$ to get $Z_T$ or $Z_K$ respectively. So we know the centralizers of both $A_T$ and $A_K$ are commutative, i.e. $Z_T^{ab} = Z_T$ and $Z_K^{ab} = Z_K$.

So we now know that $N_K/Z_K$ is a group of order 1 or 2 depending on whether there exists an element $m$ in the Galois group, such that:

$$\begin{pmatrix} z & \epsilon y \\ y & z \end{pmatrix}^m = \begin{pmatrix} z & -\epsilon y \\ -y & z \end{pmatrix}$$

We can use this result in Theorem 3.1 to get the following:

$$\begin{aligned} tors(K_1'(\mathbb{Z}_p[G_n]))_{(p)} &\cong [(\mu_F)_p]^k \oplus \bigoplus_{i=1}^k H^0(N_i/Z_i; Z_i^{ab})_{(p)} \\ &\subset \bigoplus_{i=1}^k H^0(1; Z_i^{ab})_{(p)} \\ &= \bigoplus^{p-1}(Z_I^{ab})_{(p)} \oplus \bigoplus^{\frac{(p-1)(p-2)}{2}}(Z_T^{ab})_{(p)} \oplus \bigoplus^{\frac{p(p-1)}{2}}(Z_K^{ab})_{(p)} \\ &= \bigoplus^{p-1}((\mathbb{Z}/p^n\mathbb{Z})^\times)_{(p)} \oplus \bigoplus^{\frac{(p-1)(p-2)}{2}}(Z_T)_{(p)} \oplus \bigoplus^{\frac{p(p-1)}{2}}(Z_K)_{(p)} \\ &= \bigoplus^{\frac{(p-1)(p-2)}{2}}(Z_T)_{(p)} \oplus \bigoplus^{\frac{p(p-1)}{2}}(Z_K)_{(p)} \end{aligned}$$

To simplify the expression for $SK_1(\mathbb{Z}_p[G_n])$, we need to define $H_2(Z_i)$ and $H_2^{ab}(Z_i)$. By ([6], Theorem 3.1) we know that $H_2(Z_i) \cong ker(Z_i \wedge Z_i \xrightarrow{[\cdot,\cdot]} [Z_i, Z_i])$ where $Z_i \wedge Z_i$ is the exterior product and $[Z_i, Z_i]$ is the commutator subgroup. By ([14], Chapter 8a), we have $H_2^{ab}(Z_i) = \langle g \wedge h \in H_2(Z_i) : g, h \in Z_i, gh = hg \rangle$. Therefore we have $H_2^{ab}(Z_T) = H_2(Z_T)$ and $H_2^{ab}(Z_K) = H_2(Z_K)$, therefore $H_0(N_T/Z_T; H_2(Z_T)/H_2^{ab}(Z_T)) = 1 = H_0(N_K/Z_K; H_2(Z_K)/H_2^{ab}(Z_K))$. Recall that $N_I = Z_I$:

$$\begin{aligned} SK_1(\mathbb{Z}_p[GL_2(\mathbb{Z}/p^n\mathbb{Z})]) &\cong \bigoplus_{i=1}^k H_0(N_i/Z_i; H_2(Z_i)/H_2^{ab}(Z_i))_{(p)} \\ &= \bigoplus^{p-1} H_0(N_I/Z_I; H_2(Z_I)/H_2^{ab}(Z_I))_{(p)} \\ &= \bigoplus^{p-1}(H_2(Z_I)/H_2^{ab}(Z_I))_{(p)} \\ &= \bigoplus^{p-1}(H_2(G_n)/H_2^{ab}(G_n))_{(p)} \end{aligned}$$

Although $SK_1(\mathbb{Z}_p[G_n])$ is not needed for the work done in this paper, it would be nice to compute it explicitly but we do not know how to do it.

It turns out that we can take $\mathcal{F}_n = \{Z_n, C_n, T_n, K_n, N_{t^i}, N_{k^i} | \forall i = 1, 2, ..., n-1\}$ where these subgroups are defined as follows:

$$Z_n := \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\}$$

$$C_n := \left\{ \begin{pmatrix} a & 0 \\ c & a \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ c \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

$$T_n := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\}$$

$$K_n := \left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} : \begin{array}{l} a, b \in \mathbb{Z}/p^n\mathbb{Z} \\ \text{s.t. } p \not| (a^2 - \epsilon b^2) \end{array} \right\}$$

$$N_{t^i} := \left\{ \begin{pmatrix} a & bp^i \\ b & a \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

$$N_{k^i} := \left\{ \begin{pmatrix} a & b\epsilon p^i \\ b & a \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

Our calculation of $tors(K_1'(\mathbb{Z}_p[G_n]))_{(p)}$ implies that we should included $(Z_T)_{(p)}$ and $(Z_K)_{(p)}$ in our definition of $\mathcal{F}_n$, but it turns out that we are better off using conjugates of $A_T$ and $A_K$ so we use conjugates of $Z_T$ and $Z_K$ too. These groups are $T_n$ and $K_n$ respectively; we need to use these replacement subgroups because we will conjugate[4] $A_T$ and $A_K$ to get the matrices $\begin{pmatrix} w+y & 0 \\ 0 & w-y \end{pmatrix}$

and $\begin{pmatrix} z & \epsilon y \\ y & z \end{pmatrix}$.

[4] $X^{-1}A_TX = \begin{pmatrix} w+y & 0 \\ 0 & w-y \end{pmatrix}$ and $Y^{-1}A_KY = \begin{pmatrix} z & \epsilon y \\ y & z \end{pmatrix}$ for the matrices $X^{-1} = \begin{pmatrix} 1 & y \\ -1 & y \end{pmatrix}$ and $Y = \begin{pmatrix} 0 & y \\ 1 & 0 \end{pmatrix}$. So we need to conjugate each matrix in $Z_T$ by $X^{-1}$ and each conjugate each matrix in $Z_K$ by $Y$. Doing this gives us the subgroups $T_n$ and $K_n$ respectively.

## 3.2 Conjugacy classes of $GL_2(\mathbb{Z}/p^n\mathbb{Z})$

In this section we will verify that the following table is the full table of representatives of all conjugacy classes of $GL_2(\mathbb{Z}/p^n\mathbb{Z})$:

Table 1 ([3], Table 2 and 3):

| Rep. | no. of elts per class | no. of classes |
|---|---|---|
| $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ | $1$ | $p^n - p^{n-1}$ |
| $\begin{pmatrix} x & 0 \\ 1 & x \end{pmatrix}$ | $p^{2n-2}(p^2-1)$ | $p^n - p^{n-1}$ |
| $\begin{pmatrix} w & y^2 \\ 1 & w \end{pmatrix}$ | $p^{2n-2}(p^2+p)$ | $\frac{p^{2n-2}(p-1)(p-2)}{2}$ |
| $\begin{pmatrix} z & \epsilon y^2 \\ 1 & z \end{pmatrix}$ | $p^{2n-2}(p^2-p)$ | $\frac{p^{2n-1}(p-1)}{2}$ |
| $\begin{pmatrix} x & p^i\alpha^2 \\ 1 & x \end{pmatrix}$ | $p^{2n-2}(p^2-1)$ | $\frac{p^{2n-2-i}(p-1)^2}{2}$ |
| $\begin{pmatrix} x & p^i\epsilon\alpha^2 \\ 1 & x \end{pmatrix}$ | $p^{2n-2}(p^2-1)$ | $\frac{p^{2n-2-i}(p-1)^2}{2}$ |
| $\begin{pmatrix} x & 0 \\ p^j & x \end{pmatrix}$ | $p^{2(n-1-j)}(p^2-1)$ | $p^{n-1}(p-1)$ |
| $\begin{pmatrix} x & p^i\alpha^2 \\ p^j & x \end{pmatrix}$ | $p^{2(n-1-j)}(p^2-1)$ | $\frac{p^{2n-2-i}(p-1)^2}{2}$ |
| $\begin{pmatrix} x & p^i\epsilon\alpha^2 \\ p^j & x \end{pmatrix}$ | $p^{2(n-1-j)}(p^2-1)$ | $\frac{p^{2n-2-i}(p-1)^2}{2}$ |
| $\begin{pmatrix} x & p^j\beta^2 \\ p^j & x \end{pmatrix}$ | $p^{2(n-1-j)}(p^2+p)$ | $\frac{p^{2n-2-j}(p-1)^2}{2}$ |
| $\begin{pmatrix} x & p^j\epsilon\beta^2 \\ p^j & x \end{pmatrix}$ | $p^{2(n-1-j)}(p^2-p)$ | $\frac{p^{2n-2-j}(p-1)^2}{2}$ |

$$i, j = 1, 2, ..., n-1 \text{ s.t } j < i,\ x, y \in (\mathbb{Z}/p^n\mathbb{Z})^\times \text{ and } w, z \in \mathbb{Z}/p^n\mathbb{Z} \text{ s.t } y \not\equiv \pm w\ (mod\ p)$$

$$\alpha \in (\mathbb{Z}/p^{n-i}\mathbb{Z})^\times \text{ and } \beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times$$

Here $\epsilon$ is a fixed non-square element in $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

**Theorem 3.2** *Table 1 is an exhaustive list of all conjugacy classes of $GL_2(\mathbb{Z}/p^n\mathbb{Z})$ which tells us the number of conjugacy classes of each type of matrix representative as well as the number of elements in each class.*

To prove this theorem we will verify the centralizers given in Table 2 below, and then use them to verify the 'number of elements per class'. Then we use simple counting arguments to verify the 'number of classes'. We also need to verify that the representatives give distinct classes but in most

classes this is known because the 'number of elements per class' are different. Finally we use all the information from Table 1 to confirm that this is the full list by checking the identity[5] $\sum$(no. of elts per class)(no. of classes)$= |GL_2(\mathbb{Z}/p^n\mathbb{Z})|$. This is a long process but the conjugacy classes are essential to the work done in this paper so we show the full verification.

Table 2 ([3], Table 2):

| Rep. | Centralizers | Size of Centralizers |
|---|---|---|
| $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ | $GL_2(\mathbb{Z}/p^n\mathbb{Z})$ | $p^{4n-3}(p^2-1)(p-1)$ |
| $\begin{pmatrix} x & 0 \\ 1 & x \end{pmatrix}$ | $\left\{ \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} : \begin{matrix} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{matrix} \right\}$ | $p^{2n-1}(p-1)$ |
| $\begin{pmatrix} w & y^2 \\ 1 & w \end{pmatrix}$ | $\left\{ \begin{pmatrix} a & by^2 \\ b & a \end{pmatrix} : \begin{matrix} a \in \mathbb{Z}/p^n\mathbb{Z} \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{matrix} : p \not\mid (a^2 - b^2y^2) \right\}$ | $p^{2n-2}(p-1)^2$ |
| $\begin{pmatrix} z & \epsilon y^2 \\ 1 & z \end{pmatrix}$ | $\left\{ \begin{pmatrix} a & b\epsilon y^2 \\ b & a \end{pmatrix} : \begin{matrix} a \in \mathbb{Z}/p^n\mathbb{Z} \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{matrix} : p \not\mid (a^2 - b^2\epsilon y^2) \right\}$ | $p^{2n-2}(p^2-1)$ |
| $\begin{pmatrix} x & p^i\alpha^2 \\ 1 & x \end{pmatrix}$ | $\left\{ \begin{pmatrix} a & bp^i\alpha^2 \\ b & a \end{pmatrix} : \begin{matrix} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{matrix} \right\}$ | $p^{2n-1}(p-1)$ |
| $\begin{pmatrix} x & p^i\epsilon\alpha^2 \\ 1 & x \end{pmatrix}$ | $\left\{ \begin{pmatrix} a & bp^i\epsilon\alpha^2 \\ b & a \end{pmatrix} : \begin{matrix} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{matrix} \right\}$ | $p^{2n-1}(p-1)$ |
| $\begin{pmatrix} x & 0 \\ p^j & x \end{pmatrix}$ | $\left\{ \begin{pmatrix} a & kp^{n-j} \\ b & a+lp^{n-j} \end{pmatrix} : \begin{matrix} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{matrix} \right\}$ | $p^{2n+2j-1}(p-1)$ |
| $\begin{pmatrix} x & p^i\alpha^2 \\ p^j & x \end{pmatrix}$ | $\left\{ \begin{pmatrix} a & bp^{i-j}\alpha^2 + kp^{n-j} \\ b & a+lp^{n-j} \end{pmatrix} : \begin{matrix} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{matrix} \right\}$ | $p^{2n+2j-1}(p-1)$ |
| $\begin{pmatrix} x & p^i\epsilon\alpha^2 \\ p^j & x \end{pmatrix}$ | $\left\{ \begin{pmatrix} a & bp^{i-j}\epsilon\alpha^2 + kp^{n-j} \\ b & a+lp^{n-j} \end{pmatrix} : \begin{matrix} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{matrix} \right\}$ | $p^{2n+2j-1}(p-1)$ |
| $\begin{pmatrix} x & p^j\beta^2 \\ p^j & x \end{pmatrix}$ | $\left\{ \begin{pmatrix} a & b\beta^2 + kp^{n-j} \\ b & a+lp^{n-j} \end{pmatrix} : \begin{matrix} a \in \mathbb{Z}/p^n\mathbb{Z} \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{matrix} : p \not\mid (a^2 - b^2\beta^2) \right\}$ | $p^{2(n+j-1)}(p-1)^2$ |
| $\begin{pmatrix} x & p^j\epsilon\beta^2 \\ p^j & x \end{pmatrix}$ | $\left\{ \begin{pmatrix} a & b\epsilon\beta^2 + kp^{n-j} \\ b & a+lp^{n-j} \end{pmatrix} : \begin{matrix} a \in \mathbb{Z}/p^n\mathbb{Z} \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{matrix} : p \not\mid (a^2 - b^2\epsilon\beta^2) \right\}$ | $p^{2(n+j-1)}(p^2-1)$ |

$i, j = 1, 2, ..., n-1$ s.t $j < i$, $x, y \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $w, z \in \mathbb{Z}/p^n\mathbb{Z}$ s.t $y \not\equiv \pm w \ (mod\ p)$

$k, l \in \mathbb{Z}/p^j\mathbb{Z}, \alpha \in (\mathbb{Z}/p^{n-i}\mathbb{Z})^\times$ and $\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times$

## Verifying Table 2

**Proposition 3.1** *In Table 2, the centralizers and their orders are correct.*

Before we prove this proposition, let us set up some notation:

| $A_I$ | $A_B$ | $A_T$ | $A_K$ | $A_{RT,i}$ | $A_{RK,i}$ |
|---|---|---|---|---|---|
| $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ | $\begin{pmatrix} x & 0 \\ 1 & x \end{pmatrix}$ | $\begin{pmatrix} w & y^2 \\ 1 & w \end{pmatrix}$ | $\begin{pmatrix} z & \epsilon y^2 \\ 1 & z \end{pmatrix}$ | $\begin{pmatrix} x & p^i\alpha^2 \\ 1 & x \end{pmatrix}$ | $\begin{pmatrix} x & p^i\epsilon\alpha^2 \\ 1 & x \end{pmatrix}$ |

| $A_{RB,j}$ | $A_{RBI,j,i}$ | $A_{RBJ,j,i}$ | $A_{RI,j}$ | $A_{RJ,j}$ |
|---|---|---|---|---|
| $\begin{pmatrix} x & 0 \\ p^j & x \end{pmatrix}$ | $\begin{pmatrix} x & p^i\alpha^2 \\ p^j & x \end{pmatrix}$ | $\begin{pmatrix} x & p^i\epsilon\alpha^2 \\ p^j & x \end{pmatrix}$ | $\begin{pmatrix} x & p^j\beta^2 \\ p^j & x \end{pmatrix}$ | $\begin{pmatrix} x & p^j\epsilon\beta^2 \\ p^j & x \end{pmatrix}$ |

The letters in top row represent the form[6] of the matrices under that letter.

We will conjugate each of these matrices by a generic element in $GL_2(\mathbb{Z}/p^n\mathbb{Z})$ and check that the

[5] This sum is a sum over each representation matrix.

[6] At this point we are not interested in a notation which tells us the exact matrix; we only want to know the form of matrix.

minimal conditions to fix these matrices are in fact the conditions which define the centralizer groups in Table 2. Then we check the size of these centralizer groups and use these values to verify the 'number of elements per class' stated in Table 1. This is done with a simple formula: 'number of elements per class' is equal to the order of the group, $|GL_2(\mathbb{Z}/p^n\mathbb{Z})|$ in our case, divided by the order of the centralizer group. Recall that $|GL_2(\mathbb{Z}/p^n\mathbb{Z})| = p^{4n-3}(p^2-1)(p-1)$.

**Proof of Proposition 3.1:**
We will verify each matrix representation case by case.

## Matrix $A_I$

This one is obvious since $A_I$ represents matrices in the centre of $GL_2(\mathbb{Z}/p^n\mathbb{Z})$.

## Matrix $A_B$

In this case, we want to show that the centralizer group is

$$\left\{ \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

and that this group has order $p^{2n-1}(p-1)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \cdot \begin{pmatrix} x & 0 \\ 1 & x \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{ad-bc} \begin{pmatrix} -ab + adx - bcx & -b^2 \\ a^2 & ab + adx - bcx \end{pmatrix}$$

To fix $A_B$, we need $b = 0$ for the top right corner to be zero and then we get:

$$\begin{pmatrix} x & 0 \\ a/d & x \end{pmatrix}$$

so we need just $a = d$ and we have verified the centralizer group for $A_B$.
In the centralizer group we have a choice of $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $b \in \mathbb{Z}/p^n\mathbb{Z}$ so |Centralizer Group| = $|(\mathbb{Z}/p^n\mathbb{Z})^\times||\mathbb{Z}/p^n\mathbb{Z}| = (p^n - p^{n-1})(p^n) = p^{2n-1}(p-1)$. This agrees with Table 2.
Therefore the number of elements per class= $\frac{p^{4n-3}(p^2-1)(p-1)}{p^{2n-1}(p-1)} = p^{2n-2}(p^2-1)$ which agrees with Table 1.

## Matrix $A_T$

In this case, we want to show that the centralizer group is

$$\left\{ \begin{pmatrix} a & by^2 \\ b & a \end{pmatrix} : \begin{array}{l} a \in \mathbb{Z}/p^n\mathbb{Z} \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{array} : p \not| (a^2 - b^2y^2) \right\}$$

and that this group has order $p^{2n-2}(p-1)^2$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \cdot \begin{pmatrix} w & y^2 \\ 1 & w \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{ad-bc} \begin{pmatrix} -ab + adw - bcw + cdy^2 & d^2y^2 - b^2 \\ a^2 - c^2y^2 & ab + adw - bcw - cdy^2 \end{pmatrix}$$

To fix $A_T$, we need conditions:

$$\begin{array}{rcl} w + \frac{cdy^2-ab}{ad-bc} & = & w \\ d^2y^2 - b^2 & = & (ad-bc)y^2 \\ a^2 - c^2y^2 & = & (ad-bc) \\ w - \frac{cdy^2-ab}{ad-bc} & = & w \end{array}$$

so we need:

- $d^2y^2 - b^2 = a^2y^2 - c^2y^4 = (ad-bc)y^2$
- $cdy^2 - ab = 0$

Let us split this problem into 2 different cases:

**Case** $p|d$

We need:

- $d^2y^2 - b^2 = a^2y^2 - c^2y^4 = (ad-bc)y^2$
- $cdy^2 - ab = 0$

$p$ cannot divide $b$ or $c$ so the second bullet point tells us that $p|a$. If we rearrange the first bullet point as $(d^2-a^2)y^2 = b^2 - c^2y^4$, then we can see that $b \equiv \pm cy^2 \ (mod\ p)$. Set $b = cy^2 + kp$ such that $k \in \mathbb{Z}/p^n\mathbb{Z}$. Now put this into the second bullet point:

$$cdy^2 - acy^2 - akp = 0 \iff cy^2(d-a) = akp \iff d = \frac{akp}{cy^2} + a$$

Now let's put this in the first bullet point:

$$a^2y^2 - c^2y^4 = \left(\frac{a^2kp}{cy^2} + a^2 - c^2y^2 - ckp\right)y^2$$

$$\iff 0 = \frac{a^2kp}{c} - ckpy^2$$

$$\iff c^2kpy^2 = a^2kp$$

So we need $kp = 0$. This implies that we have $b = cy^2$ and $a = d$ and with these conditions we get:

$$\frac{1}{a^2 - c^2y^2}\begin{pmatrix} w & a^2y^2 - c^2y^4 \\ a^2 - c^2y^2 & w \end{pmatrix} = \begin{pmatrix} w & y^2 \\ 1 & w \end{pmatrix}$$

This centralizer consist of matrices with which agrees with Table 2.

**Case** $p \not| d$

We need:

- $d^2y^2 - b^2 = a^2y^2 - c^2y^4 = (ad-bc)y^2$
- $cdy^2 - ab = 0$

We can rearrange the bottom bullet point into the form $c = \frac{ab}{dy^2}$. We can use this in the first bullet point:

$$\begin{aligned} & d^2y^2 - b^2 = a^2y^2 - (\tfrac{ab}{dy^2})^2y^4 = (ad - b(\tfrac{ab}{dy^2}))y^2 \\ \iff \quad & d^4y^2 - d^2b^2 = d^2a^2y^2 - a^2b^2 = ad^3y^2 - ab^2d \\ \iff \quad & d^2(d^2y^2 - b^2) = a^2(d^2y^2 - b^2) = ad(d^2y^2 - b^2) \end{aligned}$$

So $d = a$ or $b = \pm dy$. If we set $b = \pm dy$, we would have $c = \frac{\pm ady}{dy^2} = \pm\frac{a}{y}$ so we would get a matrix with determinant 0 therefore this condition gives us no matrices. If $a = d$ then $c = \frac{ab}{ay^2} = \frac{b}{y^2}$ so we have $b = cy^2$ and we saw these conditions work in the last section and these are the conditions given in Table 2.
In the centralizer group we have a choice of $a \in \mathbb{Z}/p^n\mathbb{Z}$ and $b \in \mathbb{Z}/p^n\mathbb{Z}$ but a restriction of $p \not| (a^2 - b^2y^2)$ but we can rewrite this as a choice of either:

- $a \in p(\mathbb{Z}/p^n\mathbb{Z})$ and $b \in (\mathbb{Z}/p^n\mathbb{Z})^\times$
- OR $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $b \in \mathbb{Z}/p^n\mathbb{Z}$ such that $a^2 \not\equiv b^2y^2 \ (mod\ p)$

So we get

$$\begin{aligned} & |\text{Centralizer Group}| \\ = \quad & |p(\mathbb{Z}/p^n\mathbb{Z})||\mathbb{Z}/p^n\mathbb{Z}| + |(\mathbb{Z}/p^n\mathbb{Z})^\times||(\mathbb{Z}/p^n\mathbb{Z})\backslash\{b \in \mathbb{Z}/p^n\mathbb{Z} : a^2 \equiv b^2y^2 \ (p)\}| \\ = \quad & (p^{n-1})(p^n - p^{n-1}) + (p^n - p^{n-1})(p^n - 2p^{n-1}) \\ = \quad & (p^n - p^{n-1})(p^n - p^{n-1}) = p^{2n-2}(p-1)^2 \end{aligned}$$

This agrees with Table 2.
Therefore the number of elements per class= $\frac{p^{4n-3}(p^2-1)(p-1)}{p^{2n-2}(p-1)^2} = p^{2n-1}(p+1) = p^{2n-2}(p^2+p)$ which agrees with Table 1.

## Matrix $A_K$

In this case, we want to show that the centralizer group is

$$\left\{ \begin{pmatrix} a & b\epsilon y^2 \\ b & a \end{pmatrix} : \begin{matrix} a \in \mathbb{Z}/p^n\mathbb{Z} \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{matrix} : p \not| (a^2 - b^2\epsilon y^2) \right\}$$

and that this group has order $p^{2n-2}(p^2-1)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \cdot \begin{pmatrix} z & \epsilon y^2 \\ 1 & z \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{ad - bc} \begin{pmatrix} cd\epsilon y^2 - ab - bcz + adz & d^2\epsilon y^2 - b^2 \\ a^2 - c^2\epsilon y^2 & -cd\epsilon y^2 + ab - bcz + adz \end{pmatrix}$$

This case is essentially the same as the $A_T$ case, just with $y^2$ changed for $\epsilon y^2$. This would give us the same centralizer group as the centralizer group of $A_T$ but with $y^2$ changed for $\epsilon y^2$ and this agrees with Table 2.
In the centralizer groups of matrices in the form $A_K$ we have a choice of $a \in \mathbb{Z}/p^n\mathbb{Z}$ and $b \in \mathbb{Z}/p^n\mathbb{Z}$ but a restriction of $p \not| (a^2 - b^2\epsilon y^2)$ but we can rewrite this as a choice of either:

- $a \in p(\mathbb{Z}/p^n\mathbb{Z})$ and $b \in (\mathbb{Z}/p^n\mathbb{Z})^\times$
- OR $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $b \in \mathbb{Z}/p^n\mathbb{Z}$ such that $a^2 \not\equiv b^2\epsilon y^2 \ (mod\ p)$

So we get

$$\begin{aligned} & |\text{Centralizer Group}| \\ = \; & |p(\mathbb{Z}/p^n\mathbb{Z})||\mathbb{Z}/p^n\mathbb{Z}| + |(\mathbb{Z}/p^n\mathbb{Z})^\times||(\mathbb{Z}/p^n\mathbb{Z})\backslash\{b \in \mathbb{Z}/p^n\mathbb{Z} : a^2 \equiv b^2\epsilon y^2 \ (p)\}| \\ = \; & (p^{n-1})(p^n - p^{n-1}) + (p^n - p^{n-1})(p^n) \\ = \; & (p^n - p^{n-1})(p^n + p^{n-1}) = p^{2n-2}(p^2-1) \end{aligned}$$

This agrees with Table 2.
Therefore the number of elements per class= $\frac{p^{4n-3}(p^2-1)(p-1)}{p^{2n-2}(p^2-1)} = p^{2n-1}(p-1) = p^{2n-2}(p^2-p)$ which agrees with Table 1.

## Matrix $A_{RT,i}$

In this case, we want to show that the centralizer group is

$$\left\{ \begin{pmatrix} a & bp^i\alpha^2 \\ b & a \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

and that this group has order $p^{2n-1}(p-1)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \cdot \begin{pmatrix} x & p^i\alpha^2 \\ 1 & x \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{bc-ad} \begin{pmatrix} -cd\alpha^2p^i + ab + bcx - adx & b^2 - d^2p^i\alpha^2 \\ c^2p^i\alpha^2 - a^2 & cd\alpha^2p^i - ab + bcx - adx \end{pmatrix}$$

Just like the previous section, we get the centralizer group by looking at the centralizer group of $A_T$ and changing $y^2$ for $p^i\alpha^2$, and this gives us the same centralizer group shown in Table 2.
In the centralizer group we have a choice of $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $b \in \mathbb{Z}/p^n\mathbb{Z}$ so $|\text{Centralizer Group}| = |(\mathbb{Z}/p^n\mathbb{Z})^\times||\mathbb{Z}/p^n\mathbb{Z}| = (p^n - p^{n-1})(p^n) = p^{2n-1}(p-1)$.
This agrees with Table 2.
Therefore the number of elements per class= $\frac{p^{4n-3}(p^2-1)(p-1)}{p^{2n-1}(p-1)} = p^{2n-2}(p^2-1)$ which agrees with Table 1.

## Matrix $A_{RK,i}$

In this case, we want to show that the centralizer group is

$$\left\{ \begin{pmatrix} a & bp^i\epsilon\alpha^2 \\ b & a \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

and that this group has order $p^{2n-1}(p-1)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \cdot \begin{pmatrix} x & p^i\epsilon\alpha^2 \\ 1 & x \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{bc-ad} \begin{pmatrix} -cd\epsilon\alpha^2p^i + ab + bcx - adx & b^2 - d^2p^i\epsilon\alpha^2 \\ c^2p^i\epsilon\alpha^2 - a^2 & cd\epsilon\alpha^2p^i - ab + bcx - adx \end{pmatrix}$$

Just like the previous section, we get the centralizer group by looking at the centralizer group of $A_T$ and changing $y^2$ for $p^i\epsilon\alpha^2$, and this gives us the same centralizer group shown in Table 2.
Also like the previous section we have a choice of $a \in \mathbb{Z}/p^n\mathbb{Z}$ and $b \in \mathbb{Z}/p^n\mathbb{Z}$ but a restriction of $p \not| (a^2 - b^2\epsilon y^2)$, therefore we know that

$$|\text{Centralizer Group}| = p^{2n-1}(p-1)$$

and the number of elements per class= $\frac{p^{4n-3}(p^2-1)(p-1)}{p^{2n-1}(p-1)} = p^{2n-2}(p^2-1)$ which agrees with Table 1 and Table 2.

## Matrix $A_{RB,j}$

In this case, we want to show that the centralizer group is

$$\left\{ \begin{pmatrix} a & kp^{n-j} \\ b & a+lp^{n-j} \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

and that this group has order $p^{2n+2j-1}(p-1)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \cdot \begin{pmatrix} x & 0 \\ p^j & x \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{ad-bc} \begin{pmatrix} -abp^j - bcx + adx & -b^2p^j \\ a^2p^j & abp^j - bcx + adx \end{pmatrix}$$

To fix $A_{RB,j}$, we need conditions:

$$\begin{array}{rcl} x - \frac{abp^j}{ad-bc} & = & x \\ -b^2p^j & = & 0 \\ a^2p^j & = & (ad-bc)p^j \\ x + \frac{abp^j}{ad-bc} & = & x \end{array}$$

This means that we want $p^{n-j}|b^2$ and $p^{n-j}|ab$ but we cannot have $p$ dividing both $a$ and $b$ therefore $p^{n-j}|b$. Set $b = kp^{n-j}$. We also want $a^2p^j = (ad - kp^{n-j}c)p^j = adp^j$ therefore $d = a + lp^{n-j}$. These conditions give us:

$$\frac{1}{a^2 + alp^{n-j} - ckp^{n-j}} \begin{pmatrix} a^2x + alp^{n-j}x - ckp^{n-j}x & 0 \\ a^2p^j & a^2x + alp^{n-j}x - ckp^{n-j}x \end{pmatrix}$$

$$= \begin{pmatrix} x & 0 \\ \frac{a^2p^j}{a^2+(al-ck)p^{n-j}} & x \end{pmatrix}$$

On further inspection, we find that the bottom-left entry of this matrix is $p^j$:

$$\frac{a^2p^j}{a^2 + (al-ck)p^{n-j}} = \frac{a^2p^j + 0}{a^2 + (al-ck)p^{n-j}} = \frac{a^2p^j + (al-ck)p^n}{a^2 + (al-ck)p^{n-j}} = p^j$$

Thus we have verified Table 2 shows the correct centralizer group for $A_{RB,j}$.
In the centralizer group we have a choice of $k, l \in \mathbb{Z}/p^j\mathbb{Z}$, $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $b \in \mathbb{Z}/p^n\mathbb{Z}$ so $|\text{Centralizer Group}| = |\mathbb{Z}/p^j\mathbb{Z}|^2|(\mathbb{Z}/p^n\mathbb{Z})^\times||\mathbb{Z}/p^n\mathbb{Z}| = (p^j)^2(p^n - p^{n-1})(p^n) = p^{2n+2j-1}(p-1)$. This agrees with Table 2.
Therefore the number of elements per class$= \frac{p^{4n-3}(p^2-1)(p-1)}{p^{2n+2j-1}(p-1)} = p^{2(n-1-j)}(p^2-1)$ which agrees with Table 1.

## Matrix $A_{RBI,j,i}$

In this case, we want to show that the centralizer group is

$$\left\{ \begin{pmatrix} a & bp^{i-j}\alpha^2 + kp^{n-j} \\ b & a+lp^{n-j} \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

and that this group has order $p^{2n+2j-1}(p-1)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \cdot \begin{pmatrix} x & p^i\alpha^2 \\ p^j & x \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{ad-bc} \begin{pmatrix} -abp^j + cd\alpha^2p^i - bcx + adx & -b^2p^j + d^2p^i\alpha^2 \\ -c^2p^i\alpha^2 + a^2p^j & abp^j - cd\alpha^2p^i - bcx + adx \end{pmatrix}$$

To fix $A_{RBI,j,i}$, we need conditions:

$$\begin{array}{rcl} x - \frac{abp^j - cd\alpha^2 p^i}{ad-bc} & = & x \\ d^2p^i\alpha^2 - b^2p^j & = & (ad-bc)p^i\alpha^2 \\ a^2p^j - c^2p^i\alpha^2 & = & (ad-bc)p^j \\ x + \frac{abp^j - cd\alpha^2 p^i}{ad-bc} & = & x \end{array}$$

so we need:

- $d^2p^i\alpha^2 - b^2p^j = a^2p^i\alpha^2 - c^2p^{2i-j}\alpha^4 = (ad-bc)p^i\alpha^2$
- $abp^j - cd\alpha^2p^i = 0$
- $a^2p^j - c^2p^i\alpha^2 = (ad-bc)p^j$

Like before, we will split this into 2 cases:

**Case** $p|a$

We need:

- $d^2p^i\alpha^2 - b^2p^j = a^2p^i\alpha^2 - c^2p^{2i-j}\alpha^4 = (ad-bc)p^i\alpha^2$
- $abp^j - cd\alpha^2p^i = 0$
- $a^2p^j - c^2p^i\alpha^2 = (ad-bc)p^j$

$p$ cannot divide $b$ or $c$ so we can rearrange the second bullet point as $a = \frac{cd\alpha^2}{b}p^{i-j}$. Now we plug that into the first bullet point:

$$d^2p^i\alpha^2 - b^2p^j = \frac{c^2d^2\alpha^6}{b^2}p^{3i-2j} - c^2p^{2i-j}\alpha^4 = \left(\frac{cd^2\alpha^2}{b}p^{i-j} - bc\right)p^i\alpha^2$$

$$\iff b^2d^2p^i\alpha^2 - b^4p^j = c^2d^2\alpha^6p^{3i-2j} - b^2c^2p^{2i-j}\alpha^4 = \left(bcd^2\alpha^2p^{i-j} - b^3c\right)p^i\alpha^2$$

$$\iff b^2p^j(d^2p^{i-j}\alpha^2 - b^2) = c^2\alpha^4p^{2i-j}(d^2\alpha^2p^{i-j} - b^2) = bc\alpha^2p^i\left(d^2\alpha^2p^{i-j} - b^2\right)$$

So we have either $d^2\alpha^2p^{i-j} = b^2$ or $b^2p^j = c^2\alpha^4p^{2i-j} = bc\alpha^2p^i$ but if we use the former condition, we would get a matrix with determinant zero so this condition gives us no matrices. The latter condition simplifies to $b \equiv c\alpha^2p^{i-j}\ (mod\ p^{n-j})$ and this gives us $a = \frac{d}{b}c\alpha^2p^{i-j} \equiv d\ (mod\ p^{n-j})$. Note that these conditions also satisfy the third bullet point. Set $b = c\alpha^2p^{i-j} + kp^{n-j}$ and $d = a + lp^{n-j}$, then we get:

$$\begin{pmatrix} x & \frac{-c^2\alpha^4p^{2i-j} + a^2p^i\alpha^2}{a^2 + alp^{n-j} - c^2\alpha^2p^{i-j} - ckp^{n-j}} \\ \frac{-c^2\alpha^2p^i + a^2p^j}{a^2 + alp^{n-j} - c^2\alpha^2p^{i-j} - ckp^{n-j}} & x \end{pmatrix}$$

$$= \begin{pmatrix} x & \frac{a^2p^j - c^2\alpha^2p^i}{a^2 - c^2\alpha^2p^{i-j} + (al-ck)p^{n-j}}\alpha^2p^{i-j} \\ \frac{a^2p^j - c^2\alpha^2p^i}{a^2 - c^2\alpha^2p^{i-j} + (al-ck)p^{n-j}} & x \end{pmatrix}$$

Now the top-right and bottom-left entries simplify to $\alpha^2p^i$ and $p^j$ respectively:

$$\frac{a^2p^j - c^2\alpha^2p^i}{a^2 - c^2\alpha^2p^{i-j} + (al-ck)p^{n-j}} = \frac{a^2p^j - c^2\alpha^2p^i + (al-ck)p^n}{a^2 - c^2\alpha^2p^{i-j} + (al-ck)p^{n-j}} = p^j$$

Therefore we get:

$$\begin{pmatrix} x & \alpha^2p^i \\ p^j & x \end{pmatrix}$$

So these conditions give us the same centralizer group as shown in Table 2.

**Case** $p \not| a$

We need:

- $d^2p^i\alpha^2 - b^2p^j = a^2p^i\alpha^2 - c^2p^{2i-j}\alpha^4 = (ad-bc)p^i\alpha^2$
- $abp^j - cd\alpha^2p^i = 0$
- $a^2p^j - c^2p^i\alpha^2 = (ad-bc)p^j$

We can rearrange the second bullet point as $b = \frac{cd\alpha^2}{a}p^{i-j}$. Now we plug this into the first bullet point and get:

$$d^2p^i\alpha^2 - \frac{c^2d^2\alpha^4}{a^2}p^{2i-j} = a^2p^i\alpha^2 - c^2p^{2i-j}\alpha^4 = \left(ad - \frac{c^2d\alpha^2}{a}p^{i-j}\right)p^i\alpha^2$$

$$\iff a^2d^2p^i\alpha^2 - c^2d^2\alpha^4p^{2i-j} = a^4p^i\alpha^2 - a^2c^2p^{2i-j}\alpha^4 = \left(a^3d - ac^2d\alpha^2p^{i-j}\right)p^i\alpha^2$$

$$\iff d^2p^i\alpha^2(a^2 - c^2p^{i-j}\alpha^2) = a^2p^i\alpha^2(a^2 - c^2p^{i-j}\alpha^2) = adp^i\alpha^2\left(a^2 - c^2\alpha^2p^{i-j}\right)$$

So either $a \equiv d \ (mod\ p^{n-i})$ or $a^2 = c^2p^{i-j}\alpha^2$ but the latter condition gives us no invertible matrices. By the third bullet point, we see that we must use the stricter condition of $a \equiv d \ (mod\ p^{n-j})$. With these conditions we get $b = \frac{cd\alpha^2}{a}p^{i-j} \equiv cp^{i-j}\alpha^2 \ (mod\ p^{n-j})$, so these are the same conditions we obtained in the last section so we know they give matrices in the centralizer group and they are the same conditions given in Table 2.
Like the previous case we have a choice of $k, l \in \mathbb{Z}/p^j\mathbb{Z}$, $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $b \in \mathbb{Z}/p^n\mathbb{Z}$ so $|\text{Centralizer Group}| = p^{2n+2j-1}(p-1)$. This agrees with Table 2.
Therefore the number of elements per class= $\frac{p^{4n-3}(p^2-1)(p-1)}{p^{2n+2j-1}(p-1)} = p^{2(n-1-j)}(p^2-1)$ which agrees with Table 1.

## Matrix $A_{RBJ,j,i}$

In this case, we want to show that the centralizer group is

$$\left\{ \begin{pmatrix} a & bp^{i-j}\epsilon\alpha^2 + kp^{n-j} \\ b & a + lp^{n-j} \end{pmatrix} : \begin{array}{c} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

and that this group has order $p^{2n+2j-1}(p-1)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \cdot \begin{pmatrix} x & p^i\epsilon\alpha^2 \\ p^j & x \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{bc-ad}\begin{pmatrix} abp^j - cd\epsilon\alpha^2p^i + bcx - adx & b^2p^j - d^2p^i\epsilon\alpha^2 \\ c^2p^i\epsilon\alpha^2 - a^2p^j & -abp^j + cd\epsilon\alpha^2p^i + bcx - adx \end{pmatrix}$$

This case is essentially the same as the $A_{RBI,j,i}$ case, just with $p^i\alpha^2$ changed for $p^i\epsilon\alpha^2$. This would give us the same centralizer group as the centralizer group of $A_{RBI,j,i}$ but with $p^i\alpha^2$ changed for $p^i\epsilon\alpha^2$ and this agrees with Table 2.
Also like the previous case we have a choice of $k, l \in \mathbb{Z}/p^j\mathbb{Z}$, $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $b \in \mathbb{Z}/p^n\mathbb{Z}$, therefore we know that

$$|\text{Centralizer Group}| = p^{2n+2j-1}(p-1)$$

and the number of elements per class= $\frac{p^{4n-3}(p^2-1)(p-1)}{p^{2n+2j-1}(p-1)} = p^{2(n-1-j)}(p^2-1)$ which agrees with Table 1 and Table 2.

## Matrix $A_{RI,j}$

In this case, we want to show that the centralizer group is

$$\left\{ \begin{pmatrix} a & b\beta^2 + kp^{n-j} \\ b & a + lp^{n-j} \end{pmatrix} : \begin{matrix} a \in \mathbb{Z}/p^n\mathbb{Z} \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{matrix} : p \not| (a^2 - b^2\beta^2) \right\}$$

and that this group has order $p^{2(n+j-1)}(p-1)^2$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \cdot \begin{pmatrix} x & p^j\beta^2 \\ p^j & x \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{bc - ad} \begin{pmatrix} -cd\beta^2 p^j + abp^j + bcx - adx & b^2p^j - d^2p^j\beta^2 \\ c^2p^j\beta^2 - a^2p^j & cd\beta^2p^j - abp^j + bcx - adx \end{pmatrix}$$

Just like the previous section, we get the centralizer group by looking at the centralizer group of $A_{RBI,j,i}$ and changing $p^i\alpha^2$ for $p^j\beta^2$, and this gives us the same centralizer group shown in Table 2.
In the centralizer groups of matrices in the form $A_{RI,j}$ we have a choice of $k, l \in \mathbb{Z}/p^j\mathbb{Z}$, $a \in \mathbb{Z}/p^n\mathbb{Z}$ and $b \in \mathbb{Z}/p^n\mathbb{Z}$ but a restriction of $p \not| (a^2 - b^2\beta^2)$ but we can rewrite this as a choice of $k, l \in \mathbb{Z}/p^j\mathbb{Z}$, and either:

- $a \in p(\mathbb{Z}/p^n\mathbb{Z})$ and $b \in (\mathbb{Z}/p^n\mathbb{Z})^\times$
- OR $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $b \in \mathbb{Z}/p^n\mathbb{Z}$ such that $a^2 \not\equiv b^2\beta^2 \ (mod\ p)$

So we get

$$\begin{aligned} & |\text{Centralizer Group}| \\ = \ & |\mathbb{Z}/p^j\mathbb{Z}|^2(|p(\mathbb{Z}/p^n\mathbb{Z})||\mathbb{Z}/p^n\mathbb{Z}| + |(\mathbb{Z}/p^n\mathbb{Z})^\times||(\mathbb{Z}/p^n\mathbb{Z})\backslash\{b \in \mathbb{Z}/p^n\mathbb{Z} : a^2 \equiv b^2\beta^2 \ (p)\}|) \\ = \ & (p^j)^2((p^{n-1})(p^n - p^{n-1}) + (p^n - p^{n-1})(p^n - 2p^{n-1})) \\ = \ & (p^{2j})(p^n - p^{n-1})(p^n - p^{n-1}) = p^{2(n+j-1)}(p-1)^2 \end{aligned}$$

This agrees with Table 2.
Therefore the number of elements per class= $\frac{p^{4n-3}(p^2-1)(p-1)}{p^{2(n+j-1)}(p-1)^2} = p^{2(n-1-j)}(p^2+p)$ which agrees with Table 1.

## Matrix $A_{RJ,j}$

In this case, we want to show that the centralizer group is

$$\left\{ \begin{pmatrix} a & b\epsilon\beta^2 + kp^{n-j} \\ b & a + lp^{n-j} \end{pmatrix} : \begin{matrix} a \in \mathbb{Z}/p^n\mathbb{Z} \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{matrix} : p \not| (a^2 - b^2\epsilon\beta^2) \right\}$$

and that this group has order $p^{2(n+j-1)}(p^2-1)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \cdot \begin{pmatrix} x & p^j\epsilon\beta^2 \\ p^j & x \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{bc - ad} \begin{pmatrix} -cd\epsilon\beta^2 p^j + abp^j + bcx - adx & b^2p^j - d^2p^j\epsilon\beta^2 \\ c^2p^j\epsilon\beta^2 - a^2p^j & cd\epsilon\beta^2p^j - abp^j + bcx - adx \end{pmatrix}$$

Just like the previous section, we get the centralizer group by looking at the centralizer group of $A_{RBI,j,i}$ and changing $p^i\alpha^2$ for $p^j\epsilon\beta^2$, and this gives us the same centralizer group shown in Table 2.
In the centralizer groups of matrices in the form $A_{RJ,j}$ we have a choice of $k, l \in \mathbb{Z}/p^j\mathbb{Z}$, $a \in \mathbb{Z}/p^n\mathbb{Z}$ and $b \in \mathbb{Z}/p^n\mathbb{Z}$ but a restriction of $p \not| (a^2 - b^2\epsilon\beta^2)$ but we can rewrite this as a choice of $k, l \in \mathbb{Z}/p^j\mathbb{Z}$, and either:

- $a \in p(\mathbb{Z}/p^n\mathbb{Z})$ and $b \in (\mathbb{Z}/p^n\mathbb{Z})^\times$

- OR $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $b \in \mathbb{Z}/p^n\mathbb{Z}$ such that $a^2 \not\equiv b^2\epsilon\beta^2 \ (mod\ p)$

So we get

$$\begin{array}{rl} & |\text{Centralizer Group}| \\ = & |\mathbb{Z}/p^j\mathbb{Z}|^2(|p(\mathbb{Z}/p^n\mathbb{Z})||\mathbb{Z}/p^n\mathbb{Z}| + |(\mathbb{Z}/p^n\mathbb{Z})^\times||(\mathbb{Z}/p^n\mathbb{Z})\backslash\{b \in \mathbb{Z}/p^n\mathbb{Z} : a^2 \equiv b^2\epsilon\beta^2 \ (p)\}|) \\ = & (p^j)^2((p^{n-1})(p^n - p^{n-1}) + (p^n - p^{n-1})(p^n)) \\ = & (p^{2j})(p^n - p^{n-1})(p^n + p^{n-1}) = p^{2(n+j-1)}(p^2 - 1) \end{array}$$

This agrees with Table 2.
Therefore the number of elements per class$= \frac{p^{4n-3}(p^2-1)(p-1)}{p^{2(n+j-1)}(p^2-1)} = p^{2(n-1-j)}(p^2 - p)$ which agrees with Table 1.

This concludes the proof of the proposition and we have also verified the second column in Table 1 which states the number of elements in each class.

□

## Verifying all representations generate distinct classes

**Proposition 3.2** *No representation matrix in Table 1 represent the same conjugacy classes as another representation matrix of a different form.*

**Proof:**
$A_I$ is clearly distinct from the rest. We know that most matrices do not represent the same class because they have a different "number of elements per class". So the only matrices that could give the same class are $A_B$, $A_{RT,i}$ with $A_{RK,i}$ and $A_{RB,j_0}$, $A_{RBI,j_0,i}$ with $A_{RBJ,j_0,i}$ for fixed $j_0$. All these matrices are in the form $\begin{pmatrix} t & s \\ p^m & t \end{pmatrix}$ for $s, t \in \mathbb{Z}/p^n\mathbb{Z}$ and some fixed $m = 0, 1, 2, ..., n-1$ with $p^m | s$ such that $p \not| (t^2 - sp^m)$.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \cdot \begin{pmatrix} t & s \\ p^m & t \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} t' & s' \\ p^m & t' \end{pmatrix}$$

$$\iff \frac{1}{ad-bc} \begin{pmatrix} -abp^m + cds - bct + adt & d^2s - b^2p^m \\ a^2p^m - c^2s & abp^m - cds - bct + adt \end{pmatrix} = \begin{pmatrix} t' & s' \\ p^m & t' \end{pmatrix}$$

This would mean that we would have the following equations:

$$\begin{array}{rcl} t - \frac{abp^m - cds}{ad-bc} & = & t' \\ d^2s - b^2p^m & = & (ad-bc)s' \\ a^2p^m - c^2s & = & (ad-bc)p^m \\ t + \frac{abp^m - cds}{ad-bc} & = & t' \end{array}$$

which can be rewritten as:

- $d^2s - b^2p^m = a^2s' - c^2\frac{ss'}{p^m} = (ad-bc)s'$
- $abp^m - cds = 0$
- $a^2p^m - c^2s = (ad-bc)p^m$

The second bullet point implies that $t' = t$. We will spilt this problem into 2 cases:

### Case $p|a$

We have:

- $d^2s - b^2p^m = a^2s' - c^2\frac{ss'}{p^m} = (ad - bc)s'$
- $abp^m - cds = 0$
- $a^2p^m - c^2s = (ad - bc)p^m$

$p$ does not divide $b$ and $c$ so the second bullet point can be rearranged to $a = \frac{cds}{bp^m}$. Now plug this into the first bullet point:

$$d^2s - b^2p^m = \frac{c^2d^2s^2s'}{b^2p^{2m}} - c^2\frac{ss'}{p^m} = (\frac{cd^2s}{bp^m} - bc)s'$$

$$\iff p^m(d^2\frac{s}{p^m} - b^2) = \frac{c^2ss'}{b^2p^m}(d^2\frac{s}{p^m} - b^2) = \frac{cs'}{b}(d^2\frac{s}{p^m} - b^2)$$

So we have $d^2\frac{s}{p^m} = b^2$ or $p^m = \frac{c^2ss'}{b^2p^m} = \frac{cs'}{b}$. The former condition would give a zero determinant, so we cannot conjugate by any matrix with this condition. The latter condition would give the condition $s = s'$ meaning that any matrix with this condition would be in a centralizer group and thus this would show that all representatives on Table 1 generate distinct conjugacy classes. Note that the latter condition also satisfies the third bullet point.

### Case $p \not| a$

We have:

- $d^2s - b^2p^m = a^2s' - c^2\frac{ss'}{p^m} = (ad - bc)s'$
- $abp^m - cds = 0$
- $a^2p^m - c^2s = (ad - bc)p^m$

The second bullet point can be rearranged to $b = \frac{cds}{ap^m}$. Now plug this into the first bullet point:

$$d^2s - \frac{c^2d^2s^2}{a^2p^m} = a^2s' - c^2\frac{ss'}{p^m} = (ad - \frac{c^2ds}{ap^m})s'$$

$$\iff \frac{d^2s}{a^2}(a^2 - c^2\frac{s}{p^m}) = s'(a^2 - c^2\frac{s}{p^m}) = \frac{ds'}{a}(a^2 - c^2\frac{s}{p^m})$$

So we have $c^2\frac{s}{p^m} = a^2$ or $\frac{d^2s}{a^2} = s' = \frac{ds'}{a}$. The former condition would give a zero determinant, so we cannot conjugate by any matrix with this condition. The latter condition would give the condition $s = s'$ meaning that any matrix with this condition would be in a centralizer group and thus this would show that all representatives on Table 1 do in fact generate distinct conjugacy classes. Note that the latter condition also satisfies the third bullet point.

□

## Verifying the "Number of Classes"

Recall Table 1:

| Rep. | no. of elts per class | no. of classes |
|---|---|---|
| $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ | 1 | $p^n - p^{n-1}$ |
| $\begin{pmatrix} x & 0 \\ 1 & x \end{pmatrix}$ | $p^{2n-2}(p^2-1)$ | $p^n - p^{n-1}$ |
| $\begin{pmatrix} w & y^2 \\ 1 & w \end{pmatrix}$ | $p^{2n-2}(p^2+p)$ | $\frac{p^{2n-2}(p-1)(p-2)}{2}$ |
| $\begin{pmatrix} z & \epsilon y^2 \\ 1 & z \end{pmatrix}$ | $p^{2n-2}(p^2-p)$ | $\frac{p^{2n-1}(p-1)}{2}$ |
| $\begin{pmatrix} x & p^i\alpha^2 \\ 1 & x \end{pmatrix}$ | $p^{2n-2}(p^2-1)$ | $\frac{p^{2n-2-i}(p-1)^2}{2}$ |
| $\begin{pmatrix} x & p^i\epsilon\alpha^2 \\ 1 & x \end{pmatrix}$ | $p^{2n-2}(p^2-1)$ | $\frac{p^{2n-2-i}(p-1)^2}{2}$ |
| $\begin{pmatrix} x & 0 \\ p^j & x \end{pmatrix}$ | $p^{2(n-1-j)}(p^2-1)$ | $p^{n-1}(p-1)$ |
| $\begin{pmatrix} x & p^i\alpha^2 \\ p^j & x \end{pmatrix}$ | $p^{2(n-1-j)}(p^2-1)$ | $\frac{p^{2n-2-i}(p-1)^2}{2}$ |
| $\begin{pmatrix} x & p^i\epsilon\alpha^2 \\ p^j & x \end{pmatrix}$ | $p^{2(n-1-j)}(p^2-1)$ | $\frac{p^{2n-2-i}(p-1)^2}{2}$ |
| $\begin{pmatrix} x & p^j\beta^2 \\ p^j & x \end{pmatrix}$ | $p^{2(n-1-j)}(p^2+p)$ | $\frac{p^{2n-2-j}(p-1)^2}{2}$ |
| $\begin{pmatrix} x & p^j\epsilon\beta^2 \\ p^j & x \end{pmatrix}$ | $p^{2(n-1-j)}(p^2-p)$ | $\frac{p^{2n-2-j}(p-1)^2}{2}$ |

$$i, j = 1, 2, ..., n-1 \text{ s.t } j < i,\ x, y \in (\mathbb{Z}/p^n\mathbb{Z})^\times \text{ and } w, z \in \mathbb{Z}/p^n\mathbb{Z} \text{ s.t } y \not\equiv \pm w\ (mod\ p)$$
$$\alpha \in (\mathbb{Z}/p^{n-i}\mathbb{Z})^\times \text{ and } \beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times$$

**Proposition 3.3** *In Table 1, the third column is correct which tells us the number of classes for each type of representation matrix.*

**Proof:**
To count the 'number of classes', one simply counts the different values that can be taken for each representative while taking into consideration if any class contains more than one representative, for example we look at $A_I$:

$$\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$$

We can pick $x$ as any value in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ and clearly each of these representatives gives a unique class, so the number of classes is $|(\mathbb{Z}/p^n\mathbb{Z})^\times| = p^n - p^{n-1}$. If fact, due to the proof in the previous section we do not need to worry too much about any class containing more than one or two representative; the proof in that section is general enough to be applicable to all representatives, but in that proof we did replace squared terms for $s \in \mathbb{Z}/p^n\mathbb{Z}$, so that proof does not take into account that in $A_T$, for example, $-y$ and $y$ give the same class. So the previous section tells us that no class contains more than one or two representative, depending on whether there is a squared term in the matrix or not. We will now verify, case by case, the number of classes for each matrix type:

### Matrix $A_I$

We can pick $x$ as any value in $(\mathbb{Z}/p^n\mathbb{Z})^\times$, so the number of classes is $|(\mathbb{Z}/p^n\mathbb{Z})^\times| = p^n - p^{n-1}$.

### Matrix $A_B$

We can pick $x \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, so the number of classes is $|(\mathbb{Z}/p^n\mathbb{Z})^\times| = p^n - p^{n-1}$.

### Matrix $A_T$

We can pick $y \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $w \in \mathbb{Z}/p^n\mathbb{Z}$ as long as $y \not\equiv \pm w \ (mod\ p)$. Also, the class given by $y$ is also given by $-y$, so the number of classes is $\frac{1}{2}|(\mathbb{Z}/p^n\mathbb{Z})^\times| \cdot |(\mathbb{Z}/p^n\mathbb{Z})\backslash\{w \in \mathbb{Z}/p^n\mathbb{Z} : y \equiv \pm w \ (mod\ p)\}| = \frac{1}{2}(p^n - p^{n-1})(p^n - 2p^{n-1}) = \frac{p^{2n-2}(p-1)(p-2)}{2}$.

### Matrix $A_K$

We can pick $y \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $z \in \mathbb{Z}/p^n\mathbb{Z}$. Also, the class given by $y$ is also given by $-y$, so the number of classes is $\frac{1}{2}|(\mathbb{Z}/p^n\mathbb{Z})^\times| \cdot |\mathbb{Z}/p^n\mathbb{Z}| = \frac{1}{2}(p^n - p^{n-1})(p^n) = \frac{p^{2n-1}(p-1)}{2}$.

### Matrix $A_{RT,i}$

We can pick $x \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $\alpha \in (\mathbb{Z}/p^{n-i}\mathbb{Z})^\times$. Also, the class given by $\alpha$ is also given by $-\alpha$, so the number of classes is $\frac{1}{2}|(\mathbb{Z}/p^n\mathbb{Z})^\times| \cdot |(\mathbb{Z}/p^{n-i}\mathbb{Z})^\times| = \frac{1}{2}(p^n - p^{n-1})(p^{n-i} - p^{n-i-1}) = \frac{p^{2n-2-i}(p-1)^2}{2}$.

### Matrix $A_{RK,i}$

We can pick $x \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $\alpha \in (\mathbb{Z}/p^{n-i}\mathbb{Z})^\times$. Also, the class given by $\alpha$ is also given by $-\alpha$, so the number of classes is $\frac{1}{2}|(\mathbb{Z}/p^n\mathbb{Z})^\times| \cdot |(\mathbb{Z}/p^{n-i}\mathbb{Z})^\times| = \frac{1}{2}(p^n - p^{n-1})(p^{n-i} - p^{n-i-1}) = \frac{p^{2n-2-i}(p-1)^2}{2}$.

### Matrix $A_{RB,j}$

We can pick $x \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, so the number of classes is $|(\mathbb{Z}/p^n\mathbb{Z})^\times| = p^n - p^{n-1}$.

### Matrix $A_{RBI,j,i}$ or $A_{RBJ,j,i}$

We can pick $x \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $\alpha \in (\mathbb{Z}/p^{n-i}\mathbb{Z})^\times$. Also, the class given by $\alpha$ is also given by $-\alpha$, so the number of classes is $\frac{1}{2}|(\mathbb{Z}/p^n\mathbb{Z})^\times| \cdot |(\mathbb{Z}/p^{n-i}\mathbb{Z})^\times| = \frac{1}{2}(p^n - p^{n-1})(p^{n-i} - p^{n-i-1}) = \frac{p^{2n-2-i}(p-1)^2}{2}$.

### Matrix $A_{RI,j}$ or $A_{RJ,j}$

We can pick $x \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times$. Also, the class given by $\beta$ is also given by $-\beta$, so the number of classes is $\frac{1}{2}|(\mathbb{Z}/p^n\mathbb{Z})^\times| \cdot |(\mathbb{Z}/p^{n-j}\mathbb{Z})^\times| = \frac{1}{2}(p^n - p^{n-1})(p^{n-j} - p^{n-j-1}) = \frac{p^{2n-2-j}(p-1)^2}{2}$.

□

## Verifying Table 1 is exhaustive

**Proposition 3.4** *Table 1 gives the complete list of conjugacy classes of* $GL_2(\mathbb{Z}/p^n\mathbb{Z})$.

**Proof:**
Now we must finally check the identity $\sum$(no. of elts per class)(no. of classes)$= |GL_2(\mathbb{Z}/p^n\mathbb{Z})| = p^{4n-3}(p^2-1)(p-1)$.

Recall that this sum is a sum over each representation matrix:

$$\begin{aligned}
&\textstyle\sum(\text{no. of elts per class})(\text{no. of classes})\\
= \;& p^n - p^{n-1} + p^{2n-2}(p^2-1)(p^n-p^{n-1}) + p^{2n-2}(p^2+p)\left(\tfrac{p^{2n-2}(p-1)(p-2)}{2}\right)\\
&+p^{2n-2}(p^2-p)\left(\tfrac{p^{2n-1}(p-1)}{2}\right) + \sum_i p^{2n-2}(p^2-1)\left(\tfrac{p^{2n-2-i}(p-1)^2}{2}\right)\\
&+\sum_i p^{2n-2}(p^2-1)\left(\tfrac{p^{2n-2-i}(p-1)^2}{2}\right) + \sum_j p^{2(n-1-j)}(p^2-1)\left(p^{n-1}(p-1)\right)\\
&+\sum_{j,i} p^{2(n-1-j)}(p^2-1)\left(\tfrac{p^{2n-2-i}(p-1)^2}{2}\right) + \sum_{j,i} p^{2(n-1-j)}(p^2-1)\left(\tfrac{p^{2n-2-i}(p-1)^2}{2}\right)\\
&+\sum_j p^{2(n-1-j)}(p^2+p)\left(\tfrac{p^{2n-2-j}(p-1)^2}{2}\right) + \sum_j p^{2(n-1-j)}(p^2-p)\left(\tfrac{p^{2n-2-j}(p-1)^2}{2}\right)
\end{aligned}$$

$$\begin{aligned}
= \;& p^{n-1}(p-1) + p^{3n-3}(p^2-1)(p-1) + p^{4n-3}(p^2-1)(\tfrac{p-2}{2}) + p^{4n-3}(p-1)^2(\tfrac{p}{2})\\
&+\sum_i p^{4n-4-i}(p^2-1)(p-1)^2 + \sum_j p^{3n-3-2j}(p^2-1)(p-1)\\
&+\sum_{j,i} p^{4n-4-2j-i}(p^2-1)(p-1)^2 + \sum_j p^{4n-2-3j}(p-1)^2
\end{aligned}$$

This is very messy so we will make things clearer by simplifying all the sums separately:

$$\begin{aligned}
\sum_{i=1}^{n-1} p^{4n-4-i}(p^2-1)(p-1)^2 &= p^{4n-5}(p^2-1)(p-1)^2\sum_{i=0}^{n-2} p^{-i}\\
&= p^{4n-5}(p^2-1)(p-1)^2\left(\tfrac{1-p^{1-n}}{1-p^{-1}}\right)\\
&= p^{4n-4}(p^2-1)(p-1)\\
&\quad -p^{3n-3}(p^2-1)(p-1)
\end{aligned}$$

$$\begin{aligned}
\sum_j p^{3n-3-2j}(p^2-1)(p-1) &= p^{3n-5}(p^2-1)(p-1)\left(\tfrac{1-p^{2-2n}}{1-p^{-2}}\right)\\
&= p^{3n-3}(p-1) - p^{n-1}(p-1)
\end{aligned}$$

$$\begin{aligned}
\sum_{j,i} p^{4n-4-2j-i}(p^2-1)(p-1)^2 &= p^{4n-7}(p^2-1)(p-1)^2\sum_{i=0}^{n-2} p^{-i}\sum_{j=0}^{i-1} p^{-2j}\\
&= p^{4n-7}(p^2-1)(p-1)^2\sum_{i=0}^{n-2} p^{-i}\left(\tfrac{1-p^{-2i}}{1-p^{-2}}\right)\\
&= p^{4n-5}(p-1)^2\left(\sum_{i=0}^{n-2} p^{-i} - \sum_{i=0}^{n-2} p^{-3i}\right)\\
&= p^{4n-4}(p-1) - p^{3n-3}(p-1)\\
&\quad -\tfrac{p^{4n-5}(p-1)^2(p^3-p^{6-3n})}{p^3-1}
\end{aligned}$$

$$\sum_j p^{4n-2-3j}(p-1)^2 = \tfrac{p^{4n-5}(p-1)^2(p^3-p^{6-3n})}{p^3-1}$$

Now that we have done that, we return to verifying the identity:

$$
\begin{aligned}
\therefore \quad & \textstyle\sum(\text{no. of elts per class})(\text{no. of classes}) \\
= \quad & p^{n-1}(p-1) + p^{3n-3}(p^2-1)(p-1) + \tfrac{p^{4n-3}(p-1)}{2}((p+1)(p-2)+(p-1)p) \\
& + p^{4n-4}(p^2-1)(p-1) - p^{3n-3}(p^2-1)(p-1) + p^{3n-3}(p-1) - p^{n-1}(p-1) \\
& + p^{4n-4}(p-1) - p^{3n-3}(p-1) - \tfrac{p^{4n-5}(p-1)^2(p^3-p^{6-3n})}{p^3-1} + \tfrac{p^{4n-5}(p-1)^2(p^3-p^{6-3n})}{p^3-1} \\
= \quad & (p^{n-1}(p-1) - p^{n-1}(p-1)) + (p^{3n-3}(p^2-1)(p-1) - p^{3n-3}(p^2-1)(p-1)) \\
& + p^{4n-3}(p-1)(p^2-p-1) + p^{4n-4}(p^2-1)(p-1) + p^{4n-4}(p-1) \\
& + (p^{3n-3}(p-1) - p^{3n-3}(p-1)) + (\tfrac{p^{4n-5}(p-1)^2(p^3-p^{6-3n})}{p^3-1} - \tfrac{p^{4n-5}(p-1)^2(p^3-p^{6-3n})}{p^3-1}) \\
= \quad & 0 + 0 + p^{4n-3}(p-1)(p^2-p-1) + p^{4n-4}(p^2-1)(p-1) + p^{4n-4}(p-1) + 0 + 0 \\
= \quad & p^{4n-3}(p^2-1)(p-1) - p^{4n-2}(p-1) + p^{4n-2}(p-1) - p^{4n-4}(p-1) \\
& + p^{4n-4}(p-1) \\
= \quad & p^{4n-3}(p^2-1)(p-1) = |GL_2(\mathbb{Z}/p^n\mathbb{Z})|
\end{aligned}
$$

□

With this proposition we have also proved Theorem 3.2.

## 3.3 Elements of order prime to $p$

In this section we work out the elements in $GL_2(\mathbb{Z}/p^n\mathbb{Z})$ which have order prime to $p$.
Clearly if a matrix has order prime to $p$ then any conjugate matrices also have order prime to $p$. So we inspect conjugacy classes of $GL_2(\mathbb{Z}/p^n\mathbb{Z})$:

| $A_I$ | $A_B$ | $A_T$ | $A_K$ | $A_{RT,i}$ | $A_{RK,i}$ |
|---|---|---|---|---|---|
| $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ | $\begin{pmatrix} x & 0 \\ 1 & x \end{pmatrix}$ | $\begin{pmatrix} w & y^2 \\ 1 & w \end{pmatrix}$ | $\begin{pmatrix} z & \epsilon y^2 \\ 1 & z \end{pmatrix}$ | $\begin{pmatrix} x & p^i\alpha^2 \\ 1 & x \end{pmatrix}$ | $\begin{pmatrix} x & p^i\epsilon\alpha^2 \\ 1 & x \end{pmatrix}$ |

| $A_{RB,j}$ | $A_{RBI,j,i}$ | $A_{RBJ,j,i}$ | $A_{RI,j}$ | $A_{RJ,j}$ |
|---|---|---|---|---|
| $\begin{pmatrix} x & 0 \\ p^j & x \end{pmatrix}$ | $\begin{pmatrix} x & p^i\alpha^2 \\ p^j & x \end{pmatrix}$ | $\begin{pmatrix} x & p^i\epsilon\alpha^2 \\ p^j & x \end{pmatrix}$ | $\begin{pmatrix} x & p^j\beta^2 \\ p^j & x \end{pmatrix}$ | $\begin{pmatrix} x & p^j\epsilon\beta^2 \\ p^j & x \end{pmatrix}$ |

$$i,j = 1,2,...,n-1 \text{ s.t } j<i,\ x,y \in (\mathbb{Z}/p^n\mathbb{Z})^\times \text{ and } w,z \in \mathbb{Z}/p^n\mathbb{Z} \text{ s.t } y \not\equiv \pm w \ (mod\ p)$$
$$\alpha \in (\mathbb{Z}/p^{n-i}\mathbb{Z})^\times \text{ and } \beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times$$

**Proposition 3.5** *There are only* $(p-1)(p^{2n+1}-p^{2n}-p^{2n-1}+1)$ *matrices which have order prime to* $p$. *To be precise there are* $p-1$ *matrices in the form* $A_I$, $\frac{p^{2n-1}(p^2-1)(p-2)}{2}$ *matrices conjugate to matrices in the form* $A_T$ *and* $\frac{p^{2n}(p-1)^2}{2}$ *matrices conjugate to matrices in the form* $A_K$.

**Proof:**
We will inspect each matrix representation case by case.

### Matrix $A_I$:

Clearly the order of $A_I = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ is the same as $x$, so the order of $A_I$ divides $p^n - p^{n-1}$. So $A_I$ is only prime to $p$ if the order of $x$ divides $p-1$, therefore there are precisely $p-1$ values that $x$ can take such that $A_I$ has order prime to $p$.

The identity matrix has order 1 and the rest of the matrices have order $p-1$.

### Matrix $A_B$:

$$A_B^m = \begin{pmatrix} x & 0 \\ 1 & x \end{pmatrix}^m = \begin{pmatrix} x^m & 0 \\ mx^{m-1} & x^m \end{pmatrix}$$

If $A_B^m = I_2$ then $x^m = 1$ and $mx^{m-1} = 0$, but $x \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ so $mx^{m-1} = 0$ if and only if $p^n | m$ therefore the order of $A_B$ is never prime to $p$.

### Matrix $A_T$:

$$A_T^m = \begin{pmatrix} w & y^2 \\ 1 & w \end{pmatrix}^m = \begin{pmatrix} y & y^2 \\ 1 & -y \end{pmatrix}^{-1} \begin{pmatrix} w+y & 0 \\ 0 & w-y \end{pmatrix}^m \begin{pmatrix} y & y^2 \\ 1 & -y \end{pmatrix}$$

If $A_T^m = I_2$ then $(w+y)^m = 1$ and $(w-y)^m = 1$. Set $w+y = a$ and $w+y = d$ then we get $a, d \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ such that $a \neq d$. We know there are precisely $p-1$ values $x \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ such that the order of $x$ is prime to $p$, therefore there are precisely $p-1$ values that $a$ can take and $p-2$ values that $d$ can take such that $A_T$ is prime to $p$. So there are $(p-1)(p-2)$ matrices in the form $A_T$ which have order prime to $p$. However, these values do not always give us distinct conjugacy classes; by proposition 3.3 we know that $\begin{pmatrix} w & y^2 \\ 1 & w \end{pmatrix}$ is conjugate to both $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ and $\begin{pmatrix} d & 0 \\ 0 & a \end{pmatrix}$ but no other matrices in this form. Therefore there are $\frac{(p-1)(p-2)}{2}$ conjugacy classes with representation matrices in the form $A_T$ which have order prime to $p$.

Any matrix in the form $A_T$ has order $p-1$ since at least one value, $w-y$ or $w+y$, would have order $p-1$ while the other would have order 1 or $p-1$.

### Matrix $A_K$:

Consider the projection map $GL_2(\mathbb{Z}/p^n\mathbb{Z}) \to GL_2(\mathbb{Z}/p\mathbb{Z})$. The kernal is a $p$-group of order $p^{4n-4}$ so any elements with order prime to $p$ in the $GL_2(\mathbb{Z}/p\mathbb{Z})$ will have a unique lift to an element in $GL_2(\mathbb{Z}/p^n\mathbb{Z})$ which also has order prime to $p$.

$$A_K = \begin{pmatrix} z & \epsilon y^2 \\ 1 & z \end{pmatrix}$$

Matrices in the form $A_K$ can be looked at as elements[7] in $\mathbb{F}_{p^2}^\times$ and we clearly have an injection from $\mathbb{F}_{p^2}^\times$ to $\mathbb{Z}_{p^2}^\times$. We know $\mathbb{Z}_{p^2}^\times \cong \mathbb{F}_{p^2}^\times \times P$ where $P$ is some pro-$p$ group, i.e. some group which is the inverse limit of $p$-groups so every element in $P$ has order $p$. $A_K$ maps to $x + \epsilon y \in \mathbb{Z}_{p^2}^\times$ but for $A_K$ to have order prime to $p$, we would need $x + \epsilon y \in \mathbb{F}_{p^2}^\times \times \{1\}$.

There are $p$ choices for $z$ and $p-1$ choices for $y$ that give us $x + \epsilon y \in \mathbb{F}_{p^2}^\times \times \{1\}$. Therefore there are $p(p-1)$ matrices in the form $A_K$ which have order prime to $p$. For a similar reason to the $A_T$ case, we find that there are $\frac{p(p-1)}{2}$ conjugacy classes with representation matrices in the form $A_K$ which have order prime to $p$.

All matrices in this form have order which divides $p^2 - 1$.

### Matrix $A_{RT,i}$:

If we project $A_{RT,i}$ onto $GL_2(\mathbb{Z}/p\mathbb{Z})$, we get the same matrix as the projection of $A_B$ onto $GL_2(\mathbb{Z}/p\mathbb{Z})$ and we know that the projection of $A_B$ has order divisible by $p$ thus the projection of $A_{RT,i}$ has order divisible by $p$. The order of $A_{RT,i}$ is divisible by the order of its projection, so $A_{RT,i}$ never has order prime to $p$.

### Matrix $A_{RK,i}$:

This is exactly the same strategy as $A_{RT,i}$. So $A_{RK,i}$ never has order prime to $p$.

[7] $\mathbb{F}_{p^2}$ is the finite field of $p^2$ elements and $\mathbb{Z}_{p^2}$ is as unramified extension of $\mathbb{Z}_p$ of degree 2. $\mathbb{F}_{p^2}$ can also be thought of as a degree 2 extension of $\mathbb{F}_p$ and this would make it clear how we get a natural injection from $\mathbb{F}_{p^2}^\times$ to $\mathbb{Z}_{p^2}^\times$

### Matrix $A_{RB,j}$:

Consider the projection map $GL_2(\mathbb{Z}/p^n\mathbb{Z}) \to GL_2(\mathbb{Z}/p\mathbb{Z})$. The kernal is a $p$-group of order $p^{4n-4}$ and any element of order prime to $p$ would project to an element of order prime to $p$. Therefore any elements with order prime to $p$ in the group $GL_2(\mathbb{Z}/p\mathbb{Z})$ will have a unique lift to an element in $GL_2(\mathbb{Z}/p^n\mathbb{Z})$ which also has order prime to $p$.

When projecting $A_{RB,j}$ to $GL_2(\mathbb{Z}/p\mathbb{Z})$, we get the same elements when projecting $A_I$ to $GL_2(\mathbb{Z}/p\mathbb{Z})$. So we project to matrices in the form $A_I$ which lie in $GL_2(\mathbb{Z}/p\mathbb{Z})$, but any matrix of this form which also has order prime to $p$ already lifts to a matrix in the form $A_I$ in $GL_2(\mathbb{Z}/p^n\mathbb{Z})$ which has order prime to $p$. As a result, we know that there are no elements in the form $A_{RB,j}$ which have order prime to $p$.

### Matrix $A_{RBI,j,i}$, $A_{RBJ,j,i}$, $A_{RI,j}$ or $A_{RJ,j}$:

This is exactly the same strategy as $A_{RB,j}$. So $A_{RBI,j,i}$, $A_{RBJ,j,i}$, $A_{RI,j}$ and $A_{RJ,j}$ never have order prime to $p$.

Therefore the total number of matrices which have order prime to $p$ is $\sum$(matrix reps. which have order prime to $p$)(no. of elts per conjugacy class of the matrix rep.):

$$\begin{aligned}
& p-1+\tfrac{(p-1)(p-2)}{2}\times p^{2n-2}(p^2+p)+\tfrac{p(p-1)}{2}\times p^{2n-2}(p^2-p) \\
= \quad & p-1+\tfrac{p^{2n-1}(p^2-1)(p-2)}{2}+\tfrac{p^{2n}(p-1)^2}{2} \\
= \quad & (p-1)(\tfrac{2+p^{2n-1}(p+1)(p-2)+p^{2n}(p-1)}{2}) \\
= \quad & (p-1)(\tfrac{2+p^{2n-1}(p^2-p-2+p^2-p)}{2}) \\
= \quad & (p-1)(1+p^{2n-1}(p^2-p-1)) \\
= \quad & (p-1)(p^{2n+1}-p^{2n}-p^{2n-1}+1)
\end{aligned}$$

□

# Chapter 4

# Image of $\psi_n$

Recall diagram (1) from Chapter 2.6.2:

$$\begin{array}{ccccccc} ker(Log) & \to & K_1(\mathbb{Z}_p[G_n]) & \xrightarrow{Log} & \mathbb{Z}_p[Conj(G_n)] & \to & coker(Log) \\ & & \downarrow \theta_n & & \downarrow \psi_n & & \\ ker(\mathcal{L}) & \dashrightarrow & \prod_{U\in\mathcal{F}_n} \Lambda(U^{ab})^\times & \overset{\mathcal{L}}{\dashrightarrow} & \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \prod_{U\in\mathcal{F}_n} \mathbb{Z}_p[U^{ab}] & \dashrightarrow & coker(\mathcal{L}) \end{array}$$

In the previous chapter we stated a suitable set of subgroups of $G_n$, called $\mathcal{F}_n$. In this chapter we verify that $\psi_n$ (Definition 4.1) is injective with this choice of $\mathcal{F}_n$.
After proving that $\psi_n$ is injective, we provide the image of $\psi_n$ which we call $\Psi_{n,\mathbb{Z}_p}$ (defined in Theorem 4.2). This will allow us to construct the map $\mathcal{L}$ in the next chapter.

## 4.1 Preliminaries

First recall $\mathcal{F}_n = \{Z_n, C_n, T_n, K_n, N_{t^i}, N_{k^i} | \forall i = 1, 2, ..., n-1\}$ where these subgroups are defined as follows:

$$Z_n := \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\}$$

$$C_n := \left\{ \begin{pmatrix} a & 0 \\ c & a \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ c \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

$$T_n := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\}$$

$$K_n := \left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} : \begin{array}{l} a, b \in \mathbb{Z}/p^n\mathbb{Z} \\ \text{s.t. } p \not| (a^2 - \epsilon b^2) \end{array} \right\}$$

$$N_{t^i} := \left\{ \begin{pmatrix} a & bp^i \\ b & a \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

$$N_{k^i} := \left\{ \begin{pmatrix} a & b\epsilon p^i \\ b & a \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

Next we recall the definition of $\psi_n$:

**Definition 4.1** *Let $R$ be any $\mathbb{Z}_p$-algebra of characteristic 0. For $U \in \mathcal{F}_n$, let $Tr_{G_n/U}$ be the map:*

$$\begin{array}{ccc} R[Conj(G_n)] & \to & R[Conj(U)] \\ [A]_{G_n} & \mapsto & \sum_{\substack{X \in U \backslash G_n \\ X^{-1}AX \in U}} [X^{-1}AX]_U \end{array}$$

*and let $proj_U$ be the natural projection from $R[Conj(U)]$ to $R[Conj(U^{ab})] = R[U^{ab}]$, then:*

$$\begin{array}{ccc} \psi_n : R[Conj(G_n)] & \to & \prod_{U \in \mathcal{F}_n} R[U^{ab}] \\ \psi_n : [A]_{G_n} & \mapsto & \prod_{U \in \mathcal{F}_n} proj_U \circ Tr_{G_n/U}([A]_{G_n}) \end{array}$$

**Remark:** Although this chapter concentrates on finding the image of the map $\psi_n$ in the case $R = \mathbb{Z}_p$, the results in this chapter extend to any $R$ i.e. for any $\mathbb{Z}_p$-algebra with characteristic 0, the image of the map $\psi_n$ is $\Psi_{n,R}$ (defined in Theorem 4.2).

Throughout this chapter $\psi_n$ will refer to the case $R = \mathbb{Z}_p$. By [12] we know that, when $n = 1$, we can choose $\mathcal{F}_1 = \{C_1, Z_1, T_1, K_1\}$, so $\psi_1$ is the following map:

$$\psi_1 : \mathbb{Z}_p[Conj(G_1)] \longrightarrow \mathbb{Z}_p[C_1] \times \mathbb{Z}_p[Z_1] \times \mathbb{Z}_p[T_1] \times \mathbb{Z}_p[K_1]$$

**Remark:** If we compare this choice of $\mathcal{F}_1$ and our above choice of $\mathcal{F}_n$, we notice that they coincide for $n = 1$. We also notice that the subgroups $N_{t^i}$ and $N_{k^i}$ do not appear. This is because we defined $i$ to only takes values $1, 2, ..., n-1$. In this case $n = 1$, so $i \in \emptyset$.

For each individual subgroup, we use this notation: $\psi_U := proj_U \circ Tr_{\mathcal{G}/U}([A]_{\mathcal{G}})$. This means we can write $\psi_n = \prod_{U \in \mathcal{F}_n} \psi_U$.

It will be useful if we now set up a more detailed notation to refer to the matrix representatives of the conjugacy classes of $GL_2(\mathbb{Z}/p^n\mathbb{Z})$ from section 3.2:

| $i_x$ | $c^0_{x,1}$ | $A_T$ | $A_K$ | $A_{RT,i}$ | $A_{RK,i}$ |
|---|---|---|---|---|---|
| $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ | $\begin{pmatrix} x & 0 \\ 1 & x \end{pmatrix}$ | $\begin{pmatrix} w & y^2 \\ 1 & w \end{pmatrix}$ | $\begin{pmatrix} z & \epsilon y^2 \\ 1 & z \end{pmatrix}$ | $\begin{pmatrix} x & p^i\alpha^2 \\ 1 & x \end{pmatrix}$ | $\begin{pmatrix} x & p^i\epsilon\alpha^2 \\ 1 & x \end{pmatrix}$ |

| $rc^j_{x,1}$ | $A_{RBI,j,i}$ | $A_{RBJ,j,i}$ | $A_{RI,j}$ | $A_{RJ,j}$ |
|---|---|---|---|---|
| $\begin{pmatrix} x & 0 \\ p^j & x \end{pmatrix}$ | $\begin{pmatrix} x & p^i\alpha^2 \\ p^j & x \end{pmatrix}$ | $\begin{pmatrix} x & p^i\epsilon\alpha^2 \\ p^j & x \end{pmatrix}$ | $\begin{pmatrix} x & p^j\beta^2 \\ p^j & x \end{pmatrix}$ | $\begin{pmatrix} x & p^j\epsilon\beta^2 \\ p^j & x \end{pmatrix}$ |

$$i, j = 1, 2, ..., n-1 \text{ s.t } j < i,\ x, y \in (\mathbb{Z}/p^n\mathbb{Z})^\times \text{ and } w, z \in \mathbb{Z}/p^n\mathbb{Z} \text{ s.t } y \not\equiv \pm w\ (mod\ p)$$
$$\alpha \in (\mathbb{Z}/p^{n-i}\mathbb{Z})^\times \text{ and } \beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times$$

Where $\epsilon$ is a fixed non-square element in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Set $c^0_{x,y} := \begin{pmatrix} x & 0 \\ y & x \end{pmatrix}$ and $rc^j_{x,\beta} := \begin{pmatrix} x & 0 \\ \beta p^j & x \end{pmatrix}$. Also, note that we have not set up different notation for $A_T, A_K, A_{RT,i}, A_{RK,i}, A_{RBI,j,i}, A_{RBJ,j,i} A_{RI,j}$ and $A_{RJ,j}$. This is because, from now on, it is better to use their respective conjugates

$$t^0_{w,y} := \begin{pmatrix} w+y & 0 \\ 0 & w-y \end{pmatrix} = \begin{pmatrix} 1 & y \\ -1 & y \end{pmatrix} \begin{pmatrix} w & y^2 \\ 1 & w \end{pmatrix} \begin{pmatrix} 1 & y \\ -1 & y \end{pmatrix}^{-1}$$

$$k^0_{z,y} := \begin{pmatrix} z & \epsilon y \\ y & z \end{pmatrix} = \begin{pmatrix} 0 & y \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} z & \epsilon y^2 \\ 1 & z \end{pmatrix} \begin{pmatrix} 0 & y \\ 1 & 0 \end{pmatrix}$$

$$rt^i_{x,\alpha} := \begin{pmatrix} x & p^i\alpha \\ \alpha & x \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} x & p^i\alpha^2 \\ 1 & x \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$$

$$rk^i_{x,\alpha} := \begin{pmatrix} x & p^i\epsilon\alpha \\ \alpha & x \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} x & p^i\epsilon\alpha^2 \\ 1 & x \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$$

$$rci^{j,i}_{x,\alpha} := \begin{pmatrix} x & p^i\alpha \\ p^j\alpha & x \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} x & p^i\alpha^2 \\ p^j & x \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$$

$$rcj^{j,i}_{x,\alpha} := \begin{pmatrix} x & p^i\epsilon\alpha \\ p^j\alpha & x \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} x & p^i\epsilon\alpha^2 \\ p^j & x \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$$

$$ri^j_{x,\beta} := \begin{pmatrix} x+\beta p^j & 0 \\ 0 & x-\beta p^j \end{pmatrix} = \begin{pmatrix} 1 & \beta \\ -1 & \beta \end{pmatrix} \begin{pmatrix} x & p^j\beta^2 \\ p^j & x \end{pmatrix} \begin{pmatrix} 1 & \beta \\ -1 & \beta \end{pmatrix}^{-1}$$

$$rj^j_{x,\beta} := \begin{pmatrix} x & p^j\epsilon\beta \\ p^j\beta & x \end{pmatrix} = \begin{pmatrix} 0 & \beta \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} x & p^j\epsilon\beta^2 \\ p^j & x \end{pmatrix} \begin{pmatrix} 0 & \beta \\ 1 & 0 \end{pmatrix}$$

**Remark:** The notation we use is referencing the paper [3] where we found the list of conjugacy classes of $G_n$.

## 4.2 Image of $\psi_n$

To calculate the output of each matrix under the map $\psi_n$, we need to calculate the trace maps and the projection maps. The trace maps are calculation heavy so we will leave full calculations of the trace maps in section 4.3. Since every subgroup in $\mathcal{F}_n$ is already Abelian, these projection maps are just the identity.

Here is a table of each map $\psi_U$ applied to each conjugacy class for all $U \in \mathcal{F}_n$

Table 3:

| | $\psi_{Z_n}$ | $\psi_{C_n}$ | $\psi_{T_n}$ | $\psi_{K_n}$ |
|---|---|---|---|---|
| $i_x$ | $[G_n : Z_n]i_x$ | $[G_n : C_n]i_x$ | $[G_n : T_n]i_x$ | $[G_n : K_n]i_x$ |
| $c^0_{x,1}$ | 0 | $\sum_{y\in(\mathbb{Z}/p^n\mathbb{Z})^\times} c^0_{x,y}$ | 0 | 0 |
| $t^0_{w,y}$ | 0 | 0 | $t^0_{w,y} + t^0_{w,-y}$ | 0 |
| $k^0_{z,y}$ | 0 | 0 | 0 | $k^0_{z,y} + k^0_{z,-y}$ |
| $rt^i_{x,\alpha}$ | 0 | 0 | 0 | 0 |
| $rk^i_{x,\alpha}$ | 0 | 0 | 0 | 0 |
| $rc^j_{x,1}$ | 0 | $p^{2j}\sum_{\beta\in(\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} rc^j_{x,\beta}$ | 0 | 0 |
| $rci^{j,i}_{x,\alpha}$ | 0 | 0 | 0 | 0 |
| $rcj^{j,i}_{x,\alpha}$ | 0 | 0 | 0 | 0 |
| $ri^j_{x,\beta}$ | 0 | 0 | $p^{2j}(ri^j_{x,\beta} + ri^j_{x,-\beta})$ | 0 |
| $rj^j_{x,\beta}$ | 0 | 0 | 0 | $p^{2j}(rj^j_{x,\beta} + rj^j_{x,-\beta})$ |

| | $\psi_{N_t{}^u}$ | $\psi_{N_k{}^u}$ |
|---|---|---|
| $i_x$ | $[G_n : N_t{}^u]i_x$ | $[G_n : N_k{}^u]i_x$ |
| $c^0_{x,1}$ | 0 | 0 |
| $t^0_{w,y}$ | 0 | 0 |
| $k^0_{z,y}$ | 0 | 0 |
| $rt^i_{x,\alpha}$ | $\delta_{iu}(rt^i_{x,\alpha} + rt^i_{x,-\alpha})$ | 0 |
| $rk^i_{x,\alpha}$ | 0 | $\delta_{iu}(rk^i_{x,\alpha} + rk^i_{x,-\alpha})$ |
| $rc^j_{x,1}$ | $p^{2j}\sum_{v=1}^{u+j}\delta_{vn}\left(\sum_{\beta\in(\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} rc^j_{x,\beta}\right)$ | $p^{2j}\sum_{v=1}^{u+j}\delta_{vn}\left(\sum_{\beta\in(\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} rc^j_{x,\beta}\right)$ |
| $rci^{j,i}_{x,\alpha}$ | $\delta_{(i-j)u}p^{2j}(rci^{j,i}_{x,\alpha} + rci^{j,i}_{x,-\alpha})$ | 0 |
| $rcj^{j,i}_{x,\alpha}$ | 0 | $\delta_{(i-j)u}p^{2j}(rcj^{j,i}_{x,\alpha} + rcj^{j,i}_{x,-\alpha})$ |
| $ri^j_{x,\beta}$ | 0 | 0 |
| $rj^j_{x,\beta}$ | 0 | 0 |

We want to prove that $\psi_n$ is injective and most effective and efficient way to do this seems to be constructing a left inverse for $\psi_n(Conj(G_n))$. We will call this map $\delta_n$. This map is constructed by inspection of the above table, but here we will state $\delta_n$ and then prove it is the left inverses via verification:

$$\delta_n : \prod_{U\in\mathcal{F}_n} \mathbb{Z}_p[U] \to \mathbb{Q}_p[Conj(G_n)]$$

When defining $\delta_n$, we write $U \cap Z_m$ with $U = C_n, T_n, K_n, N_{t^i}$ or $N_{k^i}$. We are using $Z_m$ to denote the pre-image of $Z_m$ from $G_m$ to $G_n$, i.e.

$$Z_m := \left\{ \begin{pmatrix} a & p^m b \\ p^m c & a + p^m d \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b, c, d \in \mathbb{Z}/p^{n-m}\mathbb{Z} \end{array} \right\}$$

Also note that $Z_n \subset U$ for any $U \in \mathcal{F}_n$, so any element $a_{Z_n} \in \mathbb{Z}_p[Z_n]$ can also be thought of as an element in $\mathbb{Z}_p[U]$.
Let $\delta_n = \sum_{U\in\mathcal{F}_n} \delta_U$ such that for any $(a_V)_{V\in\mathcal{F}_n} \in \prod_{U\in\mathcal{F}_n} \mathbb{Z}_p[U]$, we have:

$$\delta_U((a_V)) := \begin{cases} \frac{a_{Z_n}}{[G_n:Z_n]} & \text{if } U = Z_n \\ \frac{1}{[N_{G_n}(U):U]}\left(a_U - \frac{Tr_{U/U\cap Z_1}(a_U)}{[U:U\cap Z_1]}\right) & \\ + \sum_{1\le m<n} \frac{1}{[N_{G_n}(U\cap Z_m):U\cap Z_m]} & \\ \times \left(Tr_{U/U\cap Z_m}(a_U) - \frac{Tr_{U/U\cap Z_{m+1}}(a_U)}{p}\right) & \text{if } U = T_n, K_n \text{ or } C_n \\ \frac{1}{[N_{G_n}(U):U]}\left(a_U - \frac{Tr_{U/U\cap Z_1}(a_U)}{[U:U\cap Z_1]}\right) & \\ + \sum_{1\le m<n-i} \frac{1}{[N_{G_n}(U\cap Z_m):U\cap Z_m]} & \\ \times \left(Tr_{U/U\cap Z_m}(a_U) - \frac{Tr_{U/U\cap Z_{m+1}}(a_U)}{p}\right) & \text{if } U = N_{t^i} \text{ or } N_{k^i} \end{cases}$$

Such that, whenever we have groups $U \subset V$, we say $N_V(U)$ denotes the normalizer of $U$ as a subgroup of $V$.

**Theorem 4.1** $\delta_n \circ \psi_n = \mathbf{1}_{\mathbb{Z}_p[Conj(G_n)]}$

In the definition of $\delta_n$, we work out the traces of certain elements. So for each conjugacy class $[A] \in Conj(G_n)$, it will be useful to the proof of Theorem 4.1 if we know $Tr_{U/U\cap Z_m}(\psi_U([A]))$ for

$U = C_n, T_n, K_n, N_{t^i}$ or $N_{k^i}$:
We know that the image of $\psi_{C_n}$ only contains terms with matrices in the form $i_x$, $rc^j_{x,\beta}$ and $c^0_{x,y}$. So we only need to apply the trace map onto matrices in the aforementioned forms:

$$Tr_{C_n/(Z_m\cap C_n)}(A) = \begin{cases} [C_n : Z_m \cap C_n]i_x & \text{if } A = i_x \\ p^m rc^j_{x,\beta} & \text{if } A = rc^j_{x,\beta} \text{ and } j \geq m \\ 0 & \text{otherwise} \end{cases}$$

We know that the image of $\psi_{T_n}$ only contains terms with matrices in the form $i_x$, $ri^j_{x,\beta}$ and $t^0_{w,y}$:

$$Tr_{T_n/(Z_m\cap T_n)}(A) = \begin{cases} [T_n : Z_m \cap T_n]i_x & \text{if } A = i_x \\ p^{m-1}(p-1)ri^j_{x,\beta} & \text{if } A = ri^j_{x,\beta} \text{ and } j \geq m \\ 0 & \text{otherwise} \end{cases}$$

We know that the image of $\psi_{K_n}$ only contains terms with matrices in the form $i_x$, $rj^j_{x,\beta}$ and $k^0_{z,y}$:

$$Tr_{K_n/(Z_m\cap K_n)}(A) = \begin{cases} [K_n : Z_m \cap K_n]i_x & \text{if } A = i_x \\ p^{m-1}(p+1)rj^j_{x,\beta} & \text{if } A = rj^j_{x,\beta} \text{ and } j \geq m \\ 0 & \text{otherwise} \end{cases}$$

We know that the image of $\psi_{N_{t^i}}$ only contains terms with matrices in the form $i_x$, $rt^i_{x,\alpha}$, $rci^{j,i}_{x,\alpha}$ and $rc^j_{x,\beta}$:

$$Tr_{N_{t^i}/(Z_m\cap N_{t^i})}(A) = \begin{cases} [N_{t^i} : Z_m \cap N_{t^i}]i_x & \text{if } A = i_x \\ p^m rci^{j,i+j}_{x,\alpha} & \text{if } A = rci^{j,i+j}_{x,\alpha} \text{ and } j \geq m \\ p^m rc^j_{x,\beta} & \text{if } A = rc^j_{x,\beta}, i+j \geq n \text{ and } j \geq m \\ 0 & \text{otherwise} \end{cases}$$

We know that the image of $\psi_{N_{k^i}}$ only contains terms with matrices in the form $i_x$, $rk^i_{x,\alpha}$, $rcj^{j,i}_{x,\alpha}$ and $rc^j_{x,\beta}$:

$$Tr_{N_{k^i}/(Z_m\cap N_{k^i})}(A) = \begin{cases} [N_{k^i} : Z_m \cap N_{k^i}]i_x & \text{if } A = i_x \\ p^m rcj^{j,i+j}_{x,\alpha} & \text{if } A = rcj^{j,i+j}_{x,\alpha} \text{ and } j \geq m \\ p^m rc^j_{x,\beta} & \text{if } A = rc^j_{x,\beta}, i+j \geq n \text{ and } j \geq m \\ 0 & \text{otherwise} \end{cases}$$

In fact, we have $[C_n : Z_m \cap C_n] = p^m$, $[T_n : Z_m \cap T_n] = p^{m-1}(p-1)$, $[K_n : Z_m \cap K_n] = p^{m-1}(p+1)$, $[N_{t^i} : Z_m \cap N_{t^i}] = p^m$ and $[N_{k^i} : Z_m \cap N_{k^i}] = p^m$ but we have chosen to separate the case $A = i_x$ in this way because it makes the proof easier to understand. Details of these calculations can be found in section 4.3.

**Proof of Theorem 4.1:**
By definition $\delta_n \circ \psi_n = \mathbf{1}_{\mathbb{Z}_p[Conj(G_n)]}$ means that $\delta_n \circ \psi_n$ acts like the identity on $Conj(G_n)$. So we will need to verify that $\delta_U \circ \psi_n$ acts like the identity on each conjugacy class individually:

1. For $i_x$, using the table we can easily see that $\delta_{Z_n} \circ \psi_n([i_x]) = [i_x]$. To prove that $\delta_n \circ \psi_n([i_x]) = [i_x]$, we need to show that $\delta_U \circ \psi_n([i_x]) = 0$ if $U$ is not $Z_n$. From the table we know that $\psi_n([i_x]) = (a_U)_{U\in\mathcal{F}_n}$ where $a_U = [G_n : U][i_x]$. Notice that $\frac{[U:U\cap Z_{m+1}]}{p} = [U : U \cap Z_m]$ for $1 \leq m < n$. We also have $Tr_{U/U\cap Z_m}(a_U) = [U : U \cap Z_m]a_U$. Therefore we have:

$$Tr_{U/U\cap Z_m}(a_U) - \frac{Tr_{U/U\cap Z_{m+1}}(a_U)}{p} = 0$$

and

$$a_U - \frac{Tr_{U/U\cap Z_1}(a_U)}{[U : U \cap Z_1]} = 0$$

Therefore $\delta_U \circ \psi_n([i_x]) = 0$ for all $U \in \mathcal{F}_n \backslash \{Z_n\}$.

2. The cases for $rc^j_{x,1}$ and $c^0_{x,1}$ are similar so we will do $c^0_{x,1}$ and immediately do $rc^j_{x,1}$ after. For $c^0_{x,1}$, using the table we know that $\delta_U \circ \psi_n([c^0_{x,1}]) = 0$ unless $U$ is $C_n$, thus $\delta_n \circ \psi_n([c^0_{x,1}]) = \delta_{C_n} \circ \psi_n([c^0_{x,1}])$. Therefore we want to prove that $\delta_{C_n} \circ \psi_n([c^0_{x,1}]) = [c^0_{x,1}]$:
In section 4.3 we found that:

$$N_{G_n}(C_n) = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : \begin{array}{l} a, d \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ c \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

and that:

$$N_{G_n}(Z_m \cap C_n) = \left\{ \begin{pmatrix} a & b_0 p^{n-m} \\ c & d \end{pmatrix} : \begin{array}{l} a, d \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ c, b_0 \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

therefore $[N_{G_n}(C_n) : C_n] = p^{n-1}(p-1)$ and $[N_{G_n}(Z_m \cap C_n) : Z_m \cap C_n] = p^{n-1+2m}(p-1)$.
Now we can prove that $\delta_{C_n} \circ \psi_n([c^0_{x,1}]) = [c^0_{x,1}]$:

$$\begin{aligned} \delta_{C_n} \circ \psi_n([c^0_{x,1}]) &= \delta_{C_n} \left( \sum_{y \in (\mathbb{Z}/p^n\mathbb{Z})^\times} c^0_{x,y} \right) \\ &= \frac{1}{p^{n-1}(p-1)} \left( \sum_{y \in (\mathbb{Z}/p^n\mathbb{Z})^\times} [c^0_{x,y}] - 0 \right) \\ &\quad + \sum_{1 \le m < n} \frac{1}{p^{n-1+2m}(p-1)} (0-0) \\ &= \sum_{y \in (\mathbb{Z}/p^n\mathbb{Z})^\times} \frac{1}{p^{n-1}(p-1)} [c^0_{x,1}] + 0 = [c^0_{x,1}] \end{aligned}$$

Now we work on the case with matrices in the form $rc^j_{x,1}$. Like before, by looking at the table we find that $\delta_U \circ \psi_n([rc^j_{x,1}]) = 0$ if $U$ is not $C_n$, $N_{t^i}$ or $N_{k^i}$ when $i \ge n - j$. Thus we have

$$\delta_n \circ \psi_n([rc^j_{x,1}]) = \delta_{C_n} \circ \psi_n([rc^j_{x,1}]) + \sum_{i=n-j}^{n-1} (\delta_{N_{t^i}} \circ \psi_n([rc^j_{x,1}]) + \delta_{N_{k^i}} \circ \psi_n([rc^j_{x,1}]))$$

We want to show $\delta_n \circ \psi_n([rc^j_{x,1}]) = [rc^j_{x,1}]$. First we will calculate $\delta_{C_n} \circ \psi_n([rc^j_{x,1}])$:

$$\begin{aligned} &\delta_{C_n} \circ \psi_n([rc^j_{x,1}]) \\ &= \tfrac{1}{p^{n-1}(p-1)} \left( p^{2j} \sum_{\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} [rc^j_{x,\beta}] - p^{2j} \sum_{\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} [rc^j_{x,\beta}] \right) \\ &\quad + \sum_{1 \le m < j} \tfrac{1}{p^{n-1+2m}(p-1)} \left( p^{m+2j} \sum_{\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} [rc^j_{x,\beta}] - p^{m+2j} \sum_{\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} [rc^j_{x,\beta}] \right) \\ &\quad + \tfrac{1}{p^{n-1+2j}(p-1)} \left( p^{3j} \sum_{\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} [rc^j_{x,\beta}] - 0 \right) + \sum_{j < m < n} \tfrac{1}{p^{n-1+2m}(p-1)} (0-0) \\ &= \sum_{\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} \tfrac{1}{p^{n-j-1}(p-1)} [rc^j_{x,\beta}] + 0 \\ &= [rc^j_{x,1}] \end{aligned}$$

Now we will calculate $\delta_{N_{t^i}} \circ \psi_n([rc^j_{x,1}])$:

$$\begin{aligned}
&\delta_{N_{t^i}} \circ \psi_n([rc^j_{x,1}]) \\
&= \tfrac{1}{[N_{G_n}(N_{t^i}):N_{t^i}]} \left( p^{2j} \sum_{\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} [rc^j_{x,\beta}] - p^{2j} \sum_{\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} [rc^j_{x,\beta}] \right) \\
&\quad + \sum_{1 \le m < n-i} \tfrac{1}{[N_{G_n}(Z_m \cap N_{t^i}):Z_m \cap N_{t^i}]} \left( p^{m+2j} \sum_{\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} [rc^j_{x,\beta}] - p^{m+2j} \sum_{\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} [rc^j_{x,\beta}] \right) \\
&= 0
\end{aligned}$$

Note that $j$ does not appear in the sum from $m = 1$ to $n - i$ since $i \ge n - j$
This would be the same for $\delta_{N_{k^i}} \circ \psi_n([rc^j_{x,1}])$, so we will get

$$\begin{aligned}
\delta_n \circ \psi_n([rc^j_{x,1}]) &= \delta_{C_n} \circ \psi_n([rc^j_{x,1}]) + \sum_{i=n-j}^{n-1} (\delta_{N_{t^i}} \circ \psi_n([rc^j_{x,1}]) + \delta_{N_{k^i}} \circ \psi_n([rc^j_{x,1}])) \\
&= [rc^j_{x,1}] + \sum_{i=n-j}^{n-1} (0+0) \\
&= [rc^j_{x,1}]
\end{aligned}$$

3. We will mirror the previous case; looking at $t^0_{w,y}$ first and then $ri^j_{x,\beta}$. For $t^0_{w,y}$, we know that $\delta_U \circ \psi_n([t^0_{w,y}]) = 0$ unless $U$ is $T_n$, thus $\delta_n \circ \psi_n([t^0_{w,y}]) = \delta_{T_n} \circ \psi_n([t^0_{w,y}])$. So we want to show $\delta_{T_n} \circ \psi_n([t^0_{w,y}]) = [t^0_{w,y}]$:
In section 4.3 we found that:

$$N_{G_n}(T_n) = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} : a, b, c, d \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\}$$

and that $N_{G_n}(Z_m \cap T_n) =$

$$\left\{ \begin{pmatrix} a & b_0 p^{n-m} \\ c_0 p^{n-m} & d \end{pmatrix}, \begin{pmatrix} a_0 p^{n-m} & b \\ c & d_0 p^{n-m} \end{pmatrix} : \begin{array}{l} a, b, c, d \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ a_0, b_0, c_0, d_0 \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

therefore $[N_{G_n}(T_n) : T_n] = 2$ and $[N_{G_n}(Z_m \cap T_n) : Z_m \cap T_n] = 2p^{3m-1}(p-1)$. Now we can prove that $\delta_{T_n} \circ \psi_n([t^0_{w,y}]) = [t^0_{w,y}]$:

$$\begin{aligned}
\delta_{T_n} \circ \psi_n([t^0_{w,y}]) &= \delta_{T_n} \left( t^0_{w,y} + t^0_{w,-y} \right) \\
&= \frac{1}{2} \left( [t^0_{w,y}] + [t^0_{w,-y}] \right) + \sum_{1 \le m < n} \frac{1}{2p^{3m-1}(p-1)} (0) \\
&= [t^0_{w,y}]
\end{aligned}$$

For $ri^j_{x,\beta}$, we also find $\delta_n \circ \psi_n([ri^j_{x,\beta}]) = \delta_{T_n} \circ \psi_n([ri^j_{x,\beta}])$. So we want to show $\delta_{T_n} \circ \psi_n([ri^j_{x,\beta}]) = [ri^j_{x,\beta}]$:

$$\begin{aligned}
\delta_{T_n} \circ \psi_n([ri^j_{x,\beta}]) &= \frac{1}{2}(0) + \sum_{1 \le m < j} \frac{1}{2p^{3m-1}(p-1)} (0) \\
&\quad + \frac{1}{2p^{3j-1}(p-1)} \left( p^{3j-1}(p-1)([ri^j_{x,\beta}] + [ri^j_{x,-\beta}]) \right) \\
&\quad + \sum_{j < m < n} \frac{1}{2p^{3m-1}(p-1)} (0) \\
&= [ri^j_{x,\beta}]
\end{aligned}$$

4. We will mirror the previous case; looking at $k^0_{z,y}$ first and then $rj^j_{x,\beta}$. For $k^0_{z,y}$, we know that $\delta_U \circ \psi_n([k^0_{z,y}]) = 0$ unless $U$ is $K_n$, thus $\delta_n \circ \psi_n([k^0_{z,y}]) = \delta_{K_n} \circ \psi_n([k^0_{z,y}])$. So we want to show $\delta_{K_n} \circ \psi_n([k^0_{z,y}]) = [k^0_{z,y}]$:
In section 4.3 we found that:

$$N_{G_n}(K_n) = \left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix}, \begin{pmatrix} a & -\epsilon b \\ b & -a \end{pmatrix} : \begin{array}{l} a, b \in \mathbb{Z}/p^n\mathbb{Z} \\ a = 0 \implies b \neq 0 \end{array} \right\}$$

and that $N_{G_n}(Z_m \cap K_n) =$

$$\left\{ \begin{pmatrix} a & \epsilon b + kp^{n-m} \\ b & a + lp^{n-m} \end{pmatrix}, \begin{pmatrix} a & -\epsilon b + kp^{n-m} \\ b & -a + lp^{n-m} \end{pmatrix} : \begin{array}{l} a, b, k, l \in \mathbb{Z}/p^n\mathbb{Z} \\ a = 0 \implies b \neq 0 \end{array} \right\}$$

therefore $[N_{G_n}(K_n) : K_n] = 2$ and $[N_{G_n}(Z_m \cap K_n) : Z_m \cap K_n] = 2p^{3m-1}(p+1)$. Now we can prove that $\delta_{K_n} \circ \psi_n([k^0_{z,y}]) = [k^0_{z,y}]$:

$$\begin{aligned} \delta_{K_n} \circ \psi_n([k^0_{z,y}]) &= \delta_{K_n}\left(k^0_{z,y} + k^0_{z,-y}\right) \\ &= \frac{1}{2}\left([k^0_{z,y}] + [k^0_{z,-y}]\right) + \sum_{1 \leq m < n} \frac{1}{2p^{3m-1}(p+1)}(0) \\ &= [k^0_{z,y}] \end{aligned}$$

For $rj^j_{x,\beta}$, we also find $\delta_n \circ \psi_n([rj^j_{x,\beta}]) = \delta_{K_n} \circ \psi_n([rj^j_{x,\beta}])$. So we want to show $\delta_{K_n} \circ \psi_n([rj^j_{x,\beta}]) = [rj^j_{x,\beta}]$:

$$\begin{aligned} \delta_{K_n} \circ \psi_n([rj^j_{x,\beta}]) &= \frac{1}{2}(0) + \sum_{1 \leq m < j} \frac{1}{2p^{3m-1}(p+1)}(0) \\ &\quad + \frac{1}{2p^{3j-1}(p+1)}\left(p^{3j-1}(p+1)([rj^j_{x,\beta}] + [rj^j_{x,-\beta}])\right) \\ &\quad + \sum_{j < m < n} \frac{1}{2p^{3m-1}(p-1)}(0) \\ &= [rj^j_{x,\beta}] \end{aligned}$$

5. We will now do the rest of the cases, $rt^i_{x,\alpha}$, $rk^i_{x,\alpha}$, $rci^{j,i}_{x,\alpha}$ and $rcj^{j,i}_{x,\alpha}$. These cases are grouped because these matrices are in the same form, $A = \begin{pmatrix} x & \epsilon_0 p^i \alpha \\ p^j \alpha & x \end{pmatrix}$ where $0 \leq j < i < n$ and $\epsilon_0$ is either $\epsilon$, a fixed square-free element, or 1. Recall that $rt^i_{x,\alpha} \in N_{t^i}$, $rci^{j,i+j}_{x,\alpha} \in N_{t^i}$, $rk^i_{x,\alpha} \in N_{k^i}$ and $rcj^{j,i+j}_{x,\alpha} \in N_{k^i}$. We will denote the groups, $N_{t^i}$ and $N_{k^i}$ as:

$$N_A := \left\{ \begin{pmatrix} a & b\epsilon_0 p^i \\ b & a \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

where $i$ and $\epsilon_0$ are picked from the matrix $A$.
From the table, we can see that $\delta_n \circ \psi_n([A]) = \delta_{N_A} \circ \psi_n([A])$, so we need to show that $\delta_{N_A} \circ \psi_n([A]) = [A]$. In section 4.3 we found:

$$N_{G_n}(N_A) = \left\{ \begin{pmatrix} a & b\epsilon_0 p^i \\ b & a \end{pmatrix}, \begin{pmatrix} a & -b\epsilon_0 p^i \\ b & -a \end{pmatrix} \right\}$$

and that

$$N_{G_n}(Z_m \cap N_A) = \left\{ \begin{pmatrix} a & b\epsilon_0 p^{i-m} + kp^{n-m} \\ b & a + lp^{n-m} \end{pmatrix}, \begin{pmatrix} a & -b\epsilon_0 p^{i-m} + kp^{n-m} \\ b & -a + lp^{n-m} \end{pmatrix} \right\}$$

where $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, $b \in \mathbb{Z}/p^n\mathbb{Z}$ and $k, l \in \mathbb{Z}/p^j\mathbb{Z}$ such that $\alpha$, $i$, $j$ and $\epsilon_0$ are picked from the matrix $A$ and in the case that $A = rt^i_{x,\alpha}$ or $rk^i_{x,\alpha}$ we set $j = 0$. Therefore $[N_{G_n}(N_A) : N_A] = 2$ and $[N_{G_n}(Z_m \cap N_{t^i}) : Z_m \cap N_{t^i}] = 2p^{3m}$. Now we can prove that $\delta_{N_A} \circ \psi_n([A]) = [A]$:
In the case $A = rt^i_{x,\alpha}$ or $rk^i_{x,\alpha}$:

$$\begin{aligned}
\delta_{N_A} \circ \psi_n([A]) &= \delta_{N_A}\left(\begin{pmatrix} x & \epsilon_0\alpha p^i \\ \alpha & x \end{pmatrix} + \begin{pmatrix} x & -\epsilon_0\alpha p^i \\ -\alpha & x \end{pmatrix}\right) \\
&= \frac{1}{2}\left(\left[\begin{pmatrix} x & \epsilon_0\alpha p^i \\ \alpha & x \end{pmatrix}\right] + \left[\begin{pmatrix} x & -\epsilon_0\alpha p^i \\ -\alpha & x \end{pmatrix}\right]\right) \\
&\quad + \sum_{1 \le m < n-i} \frac{1}{2p^{3m}}(0) \\
&= [A]
\end{aligned}$$

In the case $A = rci^{j,i+j}_{x,\alpha}$ or $rcj^{j,i+j}_{x,\alpha}$:

$$\begin{aligned}
\delta_{N_A} \circ \psi_n([A]) &= \delta_{N_A}\left(p^{2j}\left(\begin{pmatrix} x & \epsilon_0\alpha p^{i+j} \\ \alpha p^j & x \end{pmatrix} + \begin{pmatrix} x & -\epsilon_0\alpha p^{i+j} \\ -\alpha p^j & x \end{pmatrix}\right)\right) \\
&= \frac{1}{2}(0) + \sum_{1 \le m < j} \frac{1}{2p^{3m}}(0) \\
&\quad + \frac{1}{2p^{3j}}\left(p^{3j}\left(\left[\begin{pmatrix} x & \epsilon_0\alpha p^{i+j} \\ \alpha p^j & x \end{pmatrix}\right] + \left[\begin{pmatrix} x & -\epsilon_0\alpha p^{i+j} \\ -\alpha p^j & x \end{pmatrix}\right]\right)\right) \\
&\quad + \sum_{j < m < n-i} \frac{1}{2p^{3m}}(0) \\
&= [A]
\end{aligned}$$

Note that $j$ appear in the sum from $m = 1$ to $n - i$ because if it did not, we would have $j \ge n - i$ and this condition would give us a matrix in the form $rc^j_{x,\beta}$.

□

Thus Theorem 4.1 proves that $\psi_n$ is injective for our choice of $\mathcal{F}_n$.

As mentioned in chapter 2.6.2, we want to construct the map named $\mathcal{L}$. To do this, it will be useful to describe the image of $\psi_n$:

**Theorem 4.2** *Let $R$ be a $\mathbb{Z}_p$-algebra of characteristic 0. We define $\Psi_{n,R}$ in the following way:*

1. $\Psi_{n,R} \subset p^{3n-2}R[Z_n] \times R[C_n] \times R[T_n] \times R[K_n] \times \prod_{i=1}^{n-1}(R[N_{t^i}] \times R[N_{k^i}])$
2. *For any $(a_V)_{V \in \mathcal{F}_n} \in \Psi_{n,R}$, each $a_V$ is fixed by conjugation action of $N_{G_n}(V)$*
3. *For any $(a_V)_{V \in \mathcal{F}_n} \in \Psi_{n,R}$, we have:*
   - $Tr_{V/Z_n}(a_V) = a_{Z_n}$ *for all* $V \in \mathcal{F}_n$
   - $Tr_{N_{t^i}/Z_m \cap N_{t^i}}(a_{N_{t^i}}) = Tr_{C_n/Z_m \cap C_n}(a_{C_n})$ *for* $m \ge n - i$

- $Tr_{N_{k^i}/Z_m\cap N_{k^i}}(a_{N_{k^i}}) = Tr_{C_n/Z_m\cap C_n}(a_{C_n})$ *for* $m \geq n-i$

4. *For any* $(a_V)_{V\in\mathcal{F}_n} \in \Psi_{n,R}$*, we have:*

- $Tr_{C_n/Z_m\cap C_n}(a_{C_n}) \in p^{3m}R[C_n]$
- $Tr_{T_n/Z_m\cap T_n}(a_{T_n}) \in p^{3m-1}R[T_n]$
- $Tr_{K_n/Z_m\cap K_n}(a_{K_n}) \in p^{3m-1}R[K_n]$
- $Tr_{N_{t^i}/Z_m\cap N_{t^i}}(a_{N_{t^i}}) \in p^{3m}R[N_{t^i}]$
- $Tr_{N_{k^i}/Z_m\cap N_{k^i}}(a_{N_{k^i}}) \in p^{3m}R[N_{k^i}]$

*Then* $im(\psi_n) = \Psi_{n,R}$*. So in our particular case,* $R = \mathbb{Z}_p$*, we have* $im(\psi_n) = \Psi_{n,\mathbb{Z}_p}$*.*

**Proof:**
Looking at Table 3, we can clearly see that $\psi_n$ satisfies conditions 1, 2 and 3 of $\Psi_{n,\mathbb{Z}_p}$. If we also look at $Tr_{U/U\cap Z_m}$ for $U = C_n, T_n, K_n, N_{ti}$, or $N_{k^i}$ (stated before the proof of Theorem 4.1) then we also see that $\psi_n$ satisfies condition 4 of $\Psi_{n,\mathbb{Z}_p}$ therefore $im(\psi_n)$ lies inside of $\Psi_{n,\mathbb{Z}_p}$. So to prove this theorem, we will prove that $\delta$ is injective on $\Psi_{n,\mathbb{Z}_p}$. Let $(a_V)_{V\in\mathcal{F}_n} \in \Psi_{n,\mathbb{Z}_p}$ such that $\delta_n((a_V)_{V\in\mathcal{F}_n}) = 0$. By definition of $\delta_n$, this means we have $\sum_{U\in\mathcal{F}_n}\delta_U((a_V)) = 0$. Our aim is to prove that $a_U = 0$ for each $U \in \mathcal{F}_n$:
For all $U \in \mathcal{F}_n\backslash\{Z_n\}$ we will prove that $\delta_U((a_V)) = 0$ and find an expression for $a_U$ in terms of $a_{Z_n}$. Then we will deduce that $a_{Z_n}$ is zero and as a result, we prove that $a_U = 0$ for each $U \in \mathcal{F}_n$.

Without loss of generality, set:

$$a_{C_n} = \sum_{x\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\sum_{y\in\mathbb{Z}/p^n\mathbb{Z}} a_{x,y}c^0_{x,y}$$

where $a_{x,y}$ is an element in $\mathbb{Z}_p$ and $c^0_{x,y}$ is the matrix $\begin{pmatrix} x & 0 \\ y & x \end{pmatrix}$. By point (3), we know that $Tr_{C_n/Z_n}(a_{C_n}) = a_{Z_n}$, therefore we get:

$$[C_n : Z_m\cap C_n]\sum_{x\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\sum_{y\in p^m(\mathbb{Z}/p^n\mathbb{Z})} a_{x,y}c^0_{x,y} = Tr_{C_n/Z_m\cap C_n}(a_{C_n})$$

Note that $[C_n : Z_n] = p^n$ and $[C_n : Z_m\cap C_n] = p^m$, thus we get two expressions:

$$a_{C_n} - \frac{Tr_{C_n/Z_1\cap C_n}(a_{C_n})}{[C_n : Z_1\cap C_n]} = \sum_{x\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\sum_{y\in(\mathbb{Z}/p^n\mathbb{Z})^\times} a_{x,y}c^0_{x,y}$$

and

$$Tr_{C_n/Z_m\cap C_n}(a_{C_n}) - \frac{Tr_{C_n/Z_{m+1}\cap C_n}(a_{C_n})}{p} = p^m\sum_{x\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\sum_{y\in p^m(\mathbb{Z}/p^n\mathbb{Z})^\times} a_{x,y}c^0_{x,y}$$

But we know that $c^0_{x,p^m\beta} = rc^m_{x,\beta}$. We also know that $[c^0_{x,y}] = [c^0_{x,1}]$ and $[rc^m_{x,y}] = [rc^m_{x,1}]$ for any $y \in (\mathbb{Z}/p^2\mathbb{Z})^\times$, therefore we can use point (2), from the definition of $\Psi_{n,\mathbb{Z}_p}$, to say that the coefficients $a_{x,p^my}$ are equal for different values of $y$, so we can simply write:

$$a_{C_n} - \frac{Tr_{C_n/Z_1\cap C_n}(a_{C_n})}{[C_n : Z_1\cap C_n]} = \sum_{x\in(\mathbb{Z}/p^n\mathbb{Z})^\times} a_{x,1}\sum_{y\in(\mathbb{Z}/p^n\mathbb{Z})^\times} c^0_{x,y}$$

and

$$Tr_{C_n/Z_m\cap C_n}(a_{C_n}) - \frac{Tr_{C_n/Z_{m+1}\cap C_n}(a_{C_n})}{p} = p^m\sum_{x\in(\mathbb{Z}/p^n\mathbb{Z})^\times} a_{x,p^m}\sum_{\beta\in(\mathbb{Z}/p^{n-m}\mathbb{Z})^\times} rc^m_{x,\beta}$$

Thus $\delta_{C_n}((a_V)_{V\in\mathcal{F}_n}) = \sum_{x\in(\mathbb{Z}/p^n\mathbb{Z})^\times} a_{x,1}[c^0_{x,1}] + \sum_{m=1}^{n-1} \frac{1}{p^{2m}} \sum_{x\in(\mathbb{Z}/p^n\mathbb{Z})^\times} a_{x,p^m}[rc^m_{x,1}]$. Although we are dividing by $p^{2m}$, we remain in $\mathbb{Z}_p[C_n]$ due to point (4) from the definition of $\Psi_{n,\mathbb{Z}_p}$. By the definition of $\delta_n$, we know that classes in the form $[c^0_{x,y}]$ and $[rc^m_{x,\beta}]$ can only appear in the image of $\delta_{C_n}$ (see the proof of Theorem 4.1 for details), thus, we must have $\delta_{C_n}((a_V)_{V\in\mathcal{F}_n}) = 0$. Therefore we have:

$$a_{C_n} = \frac{Tr_{C_n/Z_1\cap C_n}(a_{C_n})}{p}$$

and

$$Tr_{C_n/Z_m\cap C_n}(a_{C_n}) = \frac{Tr_{C_n/Z_{m+1}\cap C_n}(a_{C_n})}{p}$$

By point (3) and the properties of the trace map, we have $Tr_{C_n/Z_n\cap C_n}(a_{C_n}) = Tr_{C_n/Z_n}(a_{C_n}) = a_{Z_n}$. Therefore we get:

$$a_{C_n} = \frac{Tr_{C_n/Z_1\cap C_n}(a_{C_n})}{p} = \cdots = \frac{Tr_{C_n/Z_{n-1}\cap C_n}(a_{C_n})}{p^{n-1}} = \frac{a_{Z_n}}{p^n} = \frac{a_{Z_n}}{[C_n : Z_n]}$$

So we can write $a_{C_n}$ in terms of $a_{Z_n}$:

$$a_{C_n} = \frac{a_{Z_n}}{[C_n : Z_n]}$$

We can do the exact same for $T_n$ and $K_n$ to obtain $\delta_{T_n}((a_V)) = 0$, $\delta_{K_n}((a_V)) = 0$, $a_{T_n} = \frac{a_{Z_n}}{[T_n:Z_n]}$ and $a_{K_n} = \frac{a_{Z_n}}{[K_n:Z_n]}$.

We will now do the case $a_{N_{t^i}}$. Without loss of generality, set:

$$a_{N_{t^i}} = \sum_{x\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \sum_{\alpha\in\mathbb{Z}/p^n\mathbb{Z}} a_{x,\alpha} rt^i_{x,\alpha}$$

where $a_{x,\alpha}$ is an element in $\mathbb{Z}_p$ and $rt^i_{x,\alpha}$ is the matrix $\begin{pmatrix} x & p^i\alpha \\ \alpha & x \end{pmatrix}$. By following the same steps that we took for $a_{C_n}$, we get:

$$\delta_{N_{t^i}}((a_V)) = 0$$

and

$$a_{N_{t^i}} = \frac{Tr_{N_{t^i}/Z_1\cap N_{t^i}}(a_{N_{t^i}})}{p} = \cdots = \frac{Tr_{N_{t^i}/Z_{n-i}\cap N_{t^i}}(a_{N_{t^i}})}{p^{n-i}}$$

By point (3), we know that $Tr_{N_{t^i}/Z_{n-i}\cap N_{t^i}}(a_{N_{t^i}}) = Tr_{C_n/Z_{n-i}\cap C_n}(a_{C_n})$, therefore we get:

$$a_{N_{t^i}} = \frac{Tr_{C_n/Z_{n-i}\cap C_n}(a_{C_n})}{p^{n-i}} = \frac{a_{Z_n}}{[C_n : Z_n]} = \frac{a_{Z_n}}{[N_{t^i} : Z_n]}$$

We can do the same with $a_{N_{k^i}}$ to obtain $\delta_{N_{k^i}}((a_V)_{V\in\mathcal{F}_n}) = 0$ and $a_{N_{k^i}} = \frac{a_{Z_n}}{[N_{k^i}:Z_n]}$.

Recall that we have $\sum_{U\in\mathcal{F}_n} \delta_U((a_V)) = 0$, but using the above results we can deduce that $\delta_{Z_n}((a_V)) = 0$, therefore $a_{Z_n} = 0$. Throughout the proof, we have shown that for any $U \in \mathcal{F}_n$, we can write $a_U$ in terms of $a_{Z_n}$, but $a_{Z_n} = 0$, thus $a_U = 0$ for all $U \in \mathcal{F}_n$, therefore $\delta((a_V)_{V\in\mathcal{F}_n}) = 0$ if and only if $(a_V) = 0$, i.e. $\delta$ is injective. This proves that $\Psi_{n,\mathbb{Z}_p}$ is the image of $\psi_n$.

□

## 4.3 Trace maps for $G_n$

Here we give details on how to calculate the trace maps of each conjugacy class over any subgroup in $\mathcal{F}_n = \{Z_n, C_n, T_n, K_n, N_{t^i}, N_{k^i} | \forall i = 1, 2, ..., n-1\}$. Each of these subgroups have been described in chapter 4.1. We will also be calculating trace maps over the groups $Z_m \cap C_n$, $Z_m \cap T_n$, $Z_m \cap K_n$, $Z_m \cap N_{t^i}$ and $Z_m \cap N_{k^i}$ for $m = 1, 2, ..., n-1$ where $Z_m$ denotes the pre-image of $Z_m$ from $G_m$ to $G_n$, i.e.

$$Z_m := \left\{ \begin{pmatrix} a & p^m b \\ p^m c & a + p^m d \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b, c, d \in \mathbb{Z}/p^{n-m}\mathbb{Z} \end{array} \right\}$$

We define $C_m$, $T_m$, $K_m$, $N_{t^i}^{(m)}$ and $N_{k^i}^{(m)}$ in a similar way.

Throughout this section, we consider $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to be any matrix in $G_n$ and then look at $A' := X^{-1}AX$ where $A$ is a representation matrix of a conjugacy class. Whichever group, $U \in \mathcal{F}_n$, that we are taking the trace over, we will want to find every matrix $X$ such that $A'$ is in that group, $U$. After we do that, we will want to see how many of these matrices are distinct inside of $U\backslash G_n$, then it will be easy to calculate the trace: $Tr_{G_n/U}([A]_{G_n}) = \sum_{\substack{X \in U\backslash G_n \\ X^{-1}AX \in U}} [X^{-1}AX]_U$.

Whenever we have a group which contains no elements of a conjugacy class of a matrix, then the trace of that matrix over that group is zero, i.e. if $[A]_{G_n} \cap U = \emptyset$ then $Tr_{G_n/U}([A]_{G_n}) = 0$.

In this chapter we set $A' = X^{-1}AX$ and $[A]_U$ denotes the conjugacy class of $A$ as an element of $U$.

### Case $A = i_x$

Any matrix in the form $i_x$ is in the centre of $G_n$, so $A' = A$ and $i_x$ is in all the groups $U \in \mathcal{F}_n$, so for any $U \in \mathcal{F}_n$ we get the following:

$$Tr_{G_n/U}([A]_{G_n}) = \sum_{\substack{X \in U\backslash G_n \\ X^{-1}AX \in U}} [X^{-1}AX]_U = \sum_{X \in U\backslash G_n} [A]_U = [G_n : U][A]_U$$

$$= \frac{|G_n|}{|U|}[A]_U$$

### Case $A = c_{x,1}^0$ and $A = rc_{x,1}^j$

We are going to find the trace of $c_{x,1}^0$ and then find the trace of $rc_{x,1}^j$ because these cases are similar and the work done for the $A = c_{x,1}^0$ case will help us with the $A = rc_{x,1}^j$ case. For the case $A = c_{x,1}^0$, elements from $[A]_{G_n}$ are only contained in $C_n$ and no other group in $\mathcal{F}_n$, so we will have non-trivial trace only over $C_n$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} x & 0 \\ 1 & x \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{ad-bc}\begin{pmatrix} -ab+adx-bcx & -b^2 \\ a^2 & ab+adx-bcx \end{pmatrix}$$

To have this matrix, $A'$, in $C_n$, it is clear that $-b^2$ and $ab$ must be 0, so we must have $b=0$. This condition means we need $X$ in the form $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$. But now we must find out how many of these matrices are distinct in $C_n\backslash G_n$, then we can apply the trace map. To do this, we are going to take a generic element in $C_n$, multiply it by the matrix $X$ and the result will be any matrix in $C_n\backslash G_n$ which is equivalent to the matrix $X$:

$$\begin{pmatrix} x & 0 \\ y & x \end{pmatrix}\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = \begin{pmatrix} ax & 0 \\ cx+ay & dx \end{pmatrix}$$

Since $b=0$ is divisible by $p$, we know that $a$ and $d$ must be invertible. If we set $x=a^{-1}$ and $y=-ca^{-2}$ then we obtain the following:

$$\begin{pmatrix} a^{-1} & 0 \\ -ca^{-2} & a^{-1} \end{pmatrix}\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & d' \end{pmatrix}$$

where $d'=d/a$. Therefore, in $C_n\backslash G_n$, the matrices differ only by the values in the bottom right entry of the above matrix, so the trace is only going to sum over different values of $d$:

$$\begin{aligned} Tr_{G_n/C_n}([A]_{G_n}) &= \sum_{\substack{X\in C_n\backslash G_n \\ X^{-1}AX\in C_n}} [X^{-1}AX]_{C_n} = \sum_d \left[\begin{pmatrix} x & 0 \\ d^{-1} & x \end{pmatrix}\right]_{C_n} \\ &= \sum_{y\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\left[\begin{pmatrix} x & 0 \\ y & x \end{pmatrix}\right]_{C_n} = \sum_{y\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\left[c^0_{x,y}\right]_{C_n} \end{aligned}$$

In the case $A=rc^j_{x,1}$, elements from $[A]_{G_n}$ are only contained in $C_n$, $N_{t^i}$ and $N_{k^i}$ for $i\geq n-j$ and no other groups in $\mathcal{F}_n$. Elements from $[A]_{G_n}$ are also contained in $Z_m\cap C_n$, $Z_m\cap N_{t^i}$ and $Z_m\cap N_{k^i}$ for $i\geq n-j$ and $m\leq j$ but not $Z_m\cap T_n$ or $Z_m\cap K_n$, so, out of all the groups we are interested in, we will have non-trivial trace only over $C_n$, $N_{t^i}$, $N_{k^i}$, $Z_m\cap C_n$, $Z_m\cap N_{t^i}$ and $Z_m\cap N_{k^i}$ for $i\geq n-j$ and $m\leq j$. But $(Z_m\cap C_n)\subset C_n$, so we know that $Tr_{G_n/(Z_m\cap C_n)} = Tr_{C_n/(Z_m\cap C_n)}\circ Tr_{G_n/C_n}$, so once we find $Tr_{G_n/C_n}([A])$ we can calculate $Tr_{G_n/(Z_m\cap C_n)}$ by just taking the trace of $Tr_{G_n/C_n}([A])$. We also have $(Z_m\cap N_{t^i})\subset N_{t^i}$ and $(Z_m\cap N_{k^i})\subset N_{k^i}$, so we can also find $Tr_{G_n/(Z_m\cap N_{t^i})}$ and $Tr_{G_n/(Z_m\cap N_{k^i})}$ by first finding the trace of $Tr_{G_n/N_{t^i}}([A])$ and $Tr_{G_n/N_{k^i}}([A])$ respectively.

First we will find the trace over $C_n$ and $Z_m\cap C_n$ then we will do the other cases. Now we follow the same steps that we took for the case $A=c^0_{x,1}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}\begin{pmatrix} x & 0 \\ \beta p^j & x \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{ad-bc}\begin{pmatrix} -ab\beta p^j+adx-bcx & -b^2\beta p^j \\ a^2\beta p^j & ab\beta p^j+adx-bcx \end{pmatrix}$$

So $-b^2\beta p^j = 0 = ab\beta p^j$, but $p\not|\beta$ therefore $p^{n-j}|b$:

$$\begin{pmatrix} a & b_0p^{n-j} \\ c & d \end{pmatrix}^{-1}\begin{pmatrix} x & 0 \\ \beta p^j & x \end{pmatrix}\begin{pmatrix} a & b_0p^{n-j} \\ c & d \end{pmatrix} = \begin{pmatrix} x & 0 \\ \frac{a^2\beta}{ad-b_0cp^{n-j}}p^j & x \end{pmatrix}$$

Like before, we must find out how many of these matrices are distinct in $C_n\backslash G_n$:

$$\begin{pmatrix} x & 0 \\ y & x \end{pmatrix}\begin{pmatrix} a & b_0p^{n-j} \\ c & d \end{pmatrix} = \begin{pmatrix} ax & b_0p^{n-j}x \\ cx+ay & dx+b_0p^{n-j}y \end{pmatrix}$$

Since $b_0 p^{n-j}$ is divisible by $p$, we know that $a$ and $d$ must be invertible:

$$\begin{pmatrix} a^{-1} & 0 \\ -ca^{-2} & a^{-1} \end{pmatrix} \begin{pmatrix} a & b_0 p^{n-j} \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & b' p^{n-j} \\ 0 & d' \end{pmatrix}$$

where $b' = b_0/a$ and $d' = d/a - b_0 c a^{-2} p^{n-j}$:

$$\begin{aligned} Tr_{G_n/C_n}([A]_{G_n}) &= \sum_{\substack{X \in C_n \backslash G_n \\ X^{-1}AX \in C_n}} [X^{-1}AX]_{C_n} = \sum_{b,d} \left[ \begin{pmatrix} x & 0 \\ d^{-1}p^j & x \end{pmatrix} \right]_{C_n} \\ &= p^{2j} \sum_{\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} \left[ \begin{pmatrix} x & 0 \\ \beta p^j & x \end{pmatrix} \right]_{C_n} = p^{2j} \sum_{\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} \left[ r c_{x,\beta}^j \right]_{C_n} \end{aligned}$$

Now we can calculate the trace of $A$ over $Z_m \cap C_n$. We can use our previous calculation to see that, for $A \in (Z_m \cap C_n)$, we have $X^{-1}AX \in (Z_m \cap C_n)$ for any matrix $X \in C_n$.

We know $(Z_m \cap C_n)\backslash C_n = Z_m \backslash C_m$, so in $(Z_m \cap C_n)\backslash C_n$ we have $\left[ \begin{pmatrix} a & 0 \\ c & a \end{pmatrix} \right] = \left[ \begin{pmatrix} 1 & 0 \\ c' p^{n-m} & 1 \end{pmatrix} \right]$. So now we are ready to work out the trace:

$$\begin{aligned} Tr_{G_n/(Z_m \cap C_n)}([r c_{x,\beta}^j]_{G_n}) &= Tr_{C_n/(Z_m \cap C_n)} \circ Tr_{G_n/C_n}([r c_{x,\beta}^j]_{C_n}) \\ &= \sum_{\substack{X \in (Z_m \cap C_n)\backslash C_n \\ X^{-1}AX \in (Z_m \cap C_n)}} \left( p^{2j} \sum_{\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} [X^{-1} r c_{x,\beta}^j X]_{(Z_m \cap C_n)} \right) \\ &= p^{2j} \sum_c \sum_{\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} \left[ \begin{pmatrix} x & 0 \\ \beta p^j & x \end{pmatrix} \right]_{(Z_m \cap C_n)} \\ &= p^{m+2j} \sum_{\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} \left[ r c_{x,\beta}^j \right]_{(Z_m \cap C_n)} \end{aligned}$$

Now we calculate the trace of $A$ over $N_{t^i}$, $N_{k^i}$, $Z_m \cap C_n$, $Z_m \cap N_{t^i}$ and $Z_m \cap N_{k^i}$ for $i \geq n-j$ and $m \leq j$. We will denote $N_{ti}$ and $N_{k^i}$ as:

$$N_i := \left\{ \begin{pmatrix} a & b\epsilon_0 p^i \\ b & a \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

where $\epsilon_0$ is either $\epsilon$, a fixed square-free element, or 1. Now let's follow the same steps we did in the previous case:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} x & 0 \\ \beta p^j & x \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{ad - bc} \begin{pmatrix} -ab\beta p^j + adx - bcx & -b^2 \beta p^j \\ a^2 \beta p^j & ab\beta p^j + adx - bcx \end{pmatrix}$$

For this matrix to belong to $N_i$, we need $-b^2\beta p^j = a^2 \beta p^{i+j} \epsilon_0$ and $ab\beta p^j = 0$. Since $i \geq n-j$, we need $-b^2\beta p^j = 0 = ab\beta p^j$ but $p \not| \beta$ therefore $p^{n-j} | b$:

$$\begin{pmatrix} a & b_0 p^{n-j} \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} x & 0 \\ \beta p^j & x \end{pmatrix} \begin{pmatrix} a & b_0 p^{n-j} \\ c & d \end{pmatrix} = \begin{pmatrix} x & 0 \\ \frac{a^2\beta}{ad - b_0 c p^{n-j}} p^j & x \end{pmatrix}$$

Like before, we must find out how many of these matrices are distinct in $N_i \backslash G_n$:

$$\begin{pmatrix} x & \epsilon_0 y p^i \\ y & x \end{pmatrix} \begin{pmatrix} a & b_0 p^{n-j} \\ c & d \end{pmatrix} = \begin{pmatrix} ax + p^i \epsilon_0 cy & \epsilon_0 dy p^i + b_0 x p^{n-j} \\ ay + cx & dx + b_0 y p^{n-j} \end{pmatrix}$$

By choosing $x = a^{-1}(1 - c\epsilon_0 y p^i)$ and $y = -c(a^2 - c^2\epsilon_0 p^i)^{-1}$ we get the following:

$$\begin{pmatrix} x & \epsilon_0 y p^i \\ y & x \end{pmatrix}\begin{pmatrix} a & b_0 p^{n-j} \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & b' p^{n-j} \\ 0 & d' \end{pmatrix}$$

where $b' \in \mathbb{Z}/p^j\mathbb{Z}$ and $d' \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. This is the same as the last case:

$$Tr_{G_n/N_i}([A]_{G_n}) = p^{2j} \sum_{\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} \left[rc^j_{x,\beta}\right]_{N_i}$$

Now we can calculate the trace of $A$ over $Z_m \cap N_i$. We can use our previous calculation to see that, for $A \in (Z_m \cap N_i)$, we have $X^{-1}AX \in (Z_m \cap N_i)$ for any matrix $X \in N_i$ since $i \geq n - j$. We know $(Z_m \cap N_i)\backslash N_i = Z_m \backslash N_i^{(m)}$, so in $(Z_m \cap N_i)\backslash N_i$ we have $\left[\begin{pmatrix} a & p^i\epsilon_0 b \\ b & a \end{pmatrix}\right] = \left[\begin{pmatrix} 1 & p^i\epsilon_0 b' \\ b' & 1 \end{pmatrix}\right]$ where $b' \in (\mathbb{Z}/p^m\mathbb{Z})^\times$. This is also the same as the last case:

$$Tr_{G_n/(Z_m\cap N_i)}([rc^j_{x,\beta}]_{G_n}) = p^{m+2j} \sum_{\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} \left[rc^j_{x,\beta}\right]_{(Z_m \cap N_i)}$$

## Case $A = t^0_{w,y}$ and $A = ri^j_{x,\beta}$

Just like in the previous case, we find the trace of $t^0_{w,y}$ first, because it assists us with finding the trace of $ri^j_{x,\beta}$. For the case $A = t^0_{w,y}$, elements from $[A]_{G_n}$ are only contained in $T_n$, and no other group in $\mathcal{F}_n$, so we will have non-trivial trace only over $T_n$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}\begin{pmatrix} w+y & 0 \\ 0 & w-y \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{ad-bc}\begin{pmatrix} adw - bcw + bcy + ady & 2bdy \\ -2acy & adw - bcw - bcy - ady \end{pmatrix}$$

To have $A'$ in $T_n$, we need $2bdy = 0$ and $-2acy = 0$, but we also need $X$ to have non-zero determinant, so we have either both $b$ and $c$ are zero or both $a$ and $d$ are zero. This means that we either need $X = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ or $X = \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$. Now let us find how many of these elements are distinct in $T_n\backslash G_n$:

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} ax & 0 \\ 0 & dy \end{pmatrix}$$

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} = \begin{pmatrix} 0 & bx \\ cy & 0 \end{pmatrix}$$

It is clear that we can choose $x$ and $y$ in such a way that we can only pick $X$ to be two distinct matrices in $T_n\backslash G_n$:

$$\begin{pmatrix} a^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} b^{-1} & 0 \\ 0 & c^{-1} \end{pmatrix}\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

It is also clear that these two matrices are distinct.
Now it is easy to calculate the trace:

$$\begin{aligned} Tr_{G_n/T_n}([A]_{G_n}) &= \sum_{\substack{X\in T_n\backslash G_n \\ X^{-1}AX\in T_n}} [X^{-1}AX]_{T_n} \\ &= \left[\begin{pmatrix} w+y & 0 \\ 0 & w-y \end{pmatrix}\right]_{T_n} + \left[\begin{pmatrix} w-y & 0 \\ 0 & w+y \end{pmatrix}\right]_{T_n} \\ &= \left[t^0_{w,y}\right]_{T_n} + \left[t^0_{w,-y}\right]_{T_n} \end{aligned}$$

Now we look at the case $A = ri^j_{x,\beta}$. Elements from $[A]_{G_n}$ are only contained in $T_n$ and $Z_m \cap T_n$ for $m \leq j$ so we will have non-trivial trace only over $T_n$ and $Z_m \cap T_n$ for $m \leq j$. Like in the previous section, we find $Tr_{G_n/T_n}([A])$ and calculate the rest by using the fact that $Tr_{G_n/(Z_m\cap T_n)} = Tr_{T_n/(Z_m\cap T_n)} \circ Tr_{G_n/T_n}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} x+\beta p^j & 0 \\ 0 & x-\beta p^j \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{ad-bc} \begin{pmatrix} adx - bcx + ad\beta p^j + bc\beta p^j & 2bd\beta p^j \\ -2ac\beta p^j & adx - bcx - ad\beta p^j - bc\beta p^j \end{pmatrix}$$

So we either have $p^{n-j}$ divides both $b$ and $c$ or $p^{n-j}$ divides both $a$ and $d$:

$$\begin{pmatrix} a & b_0p^{n-j} \\ c_0p^{n-j} & d \end{pmatrix}^{-1} \begin{pmatrix} x+\beta p^j & 0 \\ 0 & x-\beta p^j \end{pmatrix} \begin{pmatrix} a & b_0p^{n-j} \\ c_0p^{n-j} & d \end{pmatrix}$$

$$= \begin{pmatrix} x + \frac{ad\beta}{ad-b_0c_0p^{2n-2j}}p^j & 0 \\ 0 & x - \frac{ad\beta}{ad-b_0c_0p^{2n-2j}}p^j \end{pmatrix}$$

$$\begin{pmatrix} a_0p^{n-j} & b \\ c & d_0p^{n-j} \end{pmatrix}^{-1} \begin{pmatrix} x+\beta p^j & 0 \\ 0 & x-\beta p^j \end{pmatrix} \begin{pmatrix} a_0p^{n-j} & b \\ c & d_0p^{n-j} \end{pmatrix}$$

$$= \begin{pmatrix} x + \frac{bc\beta}{a_0d_0p^{2n-2j}-bc}p^j & 0 \\ 0 & x - \frac{bc\beta}{a_0d_0p^{2n-2j}-bc}p^j \end{pmatrix}$$

Now we find out how many of these matrices are distinct in $T_n\backslash G_n$:

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \begin{pmatrix} a & b_0p^{n-j} \\ c_0p^{n-j} & d \end{pmatrix} = \begin{pmatrix} ax & b_0xp^{n-j} \\ c_0yp^{n-j} & dy \end{pmatrix}$$

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \begin{pmatrix} a_0p^{n-j} & b \\ c & d_0p^{n-j} \end{pmatrix} = \begin{pmatrix} a_0xp^{n-j} & bx \\ cy & d_0yp^{n-j} \end{pmatrix}$$

Again, it is clear that we can pick $x$ and $y$ in the following way:

$$\begin{pmatrix} a^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix} \begin{pmatrix} a & b_0p^{n-j} \\ c_0p^{n-j} & d \end{pmatrix} = \begin{pmatrix} 1 & b'p^{n-j} \\ c'p^{n-j} & 1 \end{pmatrix}$$

$$\begin{pmatrix} b^{-1} & 0 \\ 0 & c^{-1} \end{pmatrix} \begin{pmatrix} a_0p^{n-j} & b \\ c & d_0p^{n-j} \end{pmatrix} = \begin{pmatrix} a'p^{n-j} & 1 \\ 1 & d'p^{n-j} \end{pmatrix}$$

Where $a', b', c', d' \in \mathbb{Z}/p^j\mathbb{Z}$. So we get the following:

$$\begin{aligned}
Tr_{G_n/T_n}([A]_{G_n}) &= \sum_{\substack{X\in T_n\backslash G_n \\ X^{-1}AX\in T_n}} [X^{-1}AX]_{T_n} \\
&= \sum_{b,c}\left[\begin{pmatrix} x+\frac{\beta}{1-bcp^{2n-2j}}p^j & 0 \\ 0 & x-\frac{\beta}{1-bcp^{2n-2j}}p^j \end{pmatrix}\right]_{T_n} \\
&\quad +\sum_{a,d}\left[\begin{pmatrix} x+\frac{\beta}{adp^{2n-2j}-1}p^j & 0 \\ 0 & x-\frac{\beta}{adp^{2n-2j}-1}p^j \end{pmatrix}\right]_{T_n} \\
&= \sum_{b,c}\left[\begin{pmatrix} x+\beta p^j & 0 \\ 0 & x-\beta p^j \end{pmatrix}\right]_{T_n} + \sum_{a,d}\left[\begin{pmatrix} x-\beta p^j & 0 \\ 0 & x+\beta p^j \end{pmatrix}\right]_{T_n} \\
&= p^{2j}\left[ri^j_{x,\beta}\right]_{T_n} + p^{2j}\left[ri^j_{x,-\beta}\right]_{T_n}
\end{aligned}$$

Now we can calculate the trace of $A$ over $Z_m \cap T_n$. Like the previous section, we use our previous calculation to see that, for $A \in (Z_m \cap T_n)$, we always have $X^{-1}AX \in (Z_m \cap T_n)$ for any $X \in T_n$. We know $(Z_m \cap T_n)\backslash T_n = Z_m\backslash T_m$, so in $(Z_m \cap T_n)\backslash T_n$ we have $\left[\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\right] = \left[\begin{pmatrix} 1 & 0 \\ 0 & d' \end{pmatrix}\right]$ where $d' \in (\mathbb{Z}/p^m\mathbb{Z})^\times$. So now we are ready to work out the trace:

$$\begin{aligned}
Tr_{G_n/(Z_m\cap T_n)}([ri^j_{x,\beta}]_{G_n}) &= \sum_{\substack{X\in(Z_m\cap T_n)\backslash T_n \\ X^{-1}AX\in(Z_m\cap T_n)}} p^{2j}[X^{-1}ri^j_{x,\beta}X]_{(Z_m\cap T_n)} \\
&\quad + \sum_{\substack{X\in(Z_m\cap T_n)\backslash T_n \\ X^{-1}AX\in(Z_m\cap T_n)}} p^{2j}[X^{-1}ri^j_{x,-\beta}X]_{(Z_m\cap T_n)} \\
&= \sum_d p^{2j}\left[\begin{pmatrix} x+\beta p^j & 0 \\ 0 & x-\beta p^j \end{pmatrix}\right]_{(Z_m\cap T_n)} \\
&\quad +\sum_d p^{2j}\left[\begin{pmatrix} x-\beta p^j & 0 \\ 0 & x+\beta p^j \end{pmatrix}\right]_{(Z_m\cap T_n)} \\
&= p^{m+2j-1}(p-1)\left(\left[ri^j_{x,\beta}\right]_{(Z_m\cap T_n)} + \left[ri^j_{x,-\beta}\right]_{(Z_m\cap T_n)}\right)
\end{aligned}$$

## Case $A = k^0_{z,y}$ and $A = rj^j_{x,\beta}$

Just like in the previous cases, we find the trace of $k^0_{z,y}$ first. For the case $A = k^0_{z,y}$, elements from $[A]_{G_n}$ are only contained in $K_n$, and no other group in $\mathcal{F}_n$, so we will have non-trivial trace only over $K_n$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}\begin{pmatrix} z & \epsilon y \\ y & z \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{ad-bc}\begin{pmatrix} adx-bcx-aby+cd\epsilon y & d^2\epsilon y - b^2 y \\ a^2y - c^2\epsilon y & adz-bcz+aby-cd\epsilon y \end{pmatrix}$$

To find the conditions on $X$ such that $A' \in K_n$, we need equate $A'$ to a generic term in $K_n$, i.e. $\begin{pmatrix} w & \epsilon x \\ x & w \end{pmatrix}$ where $x, w \in \mathbb{Z}/p^n\mathbb{Z}$ such that $w^2 - \epsilon x^2 \neq 0$. So we have the following conditions:

- $d^2\epsilon y - b^2 y = (ad-bc)\epsilon x$
- $a^2 y - c^2\epsilon y = (ad-bc)x$
- $aby - cd\epsilon y = 0$

It turns out that these conditions imply that we have $a = d$ and $b = \epsilon c$ or that we have $a = -d$ and $c = -\epsilon b$. We are just stating this result for now but we will prove a more general result below. This means that we either need $X = \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix}$ or $X = \begin{pmatrix} a & -\epsilon b \\ b & -a \end{pmatrix}$. Now let us find how many of these elements are distinct in $K_n \backslash G_n$:

$$\begin{pmatrix} z & \epsilon y \\ y & z \end{pmatrix} \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} = \begin{pmatrix} az + \epsilon by & \epsilon(ay + bz) \\ ay + bz & az + \epsilon by \end{pmatrix}$$

$$\begin{pmatrix} z & \epsilon y \\ y & z \end{pmatrix} \begin{pmatrix} a & -\epsilon b \\ b & -a \end{pmatrix} = \begin{pmatrix} az + \epsilon by & -\epsilon(ay + bz) \\ ay + bz & -(az + \epsilon by) \end{pmatrix}$$

Since $\begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix}$ is in $K_n$ and $\begin{pmatrix} a & -\epsilon b \\ b & -a \end{pmatrix}$ is not, it is clear that these two are distinct in $K_n \backslash G_n$. This also means that we can simply choose $\begin{pmatrix} z & \epsilon y \\ y & z \end{pmatrix} = \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix}^{-1}$ and this would give us a $z + \epsilon by = 1$ and $ay + bz = 0$:

$$\begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix}^{-1} \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix}^{-1} \begin{pmatrix} a & -\epsilon b \\ b & -a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Now it is easy to compute the trace:

$$\begin{aligned} Tr_{G_n/K_n}([A]_{G_n}) &= \sum_{\substack{X \in K_n \backslash G_n \\ X^{-1}AX \in K_n}} [X^{-1}AX]_{K_n} \\ &= \left[ \begin{pmatrix} z & \epsilon y \\ y & z \end{pmatrix} \right]_{K_n} + \left[ \begin{pmatrix} z & -\epsilon y \\ -y & z \end{pmatrix} \right]_{K_n} \\ &= \left[k^0_{z,y}\right]_{K_n} + \left[k^0_{z,-y}\right]_{K_n} \end{aligned}$$

Now we look at the case $A = rj^j_{x,\beta}$. Elements from $[A]_{G_n}$ are only contained in $K_n$ and $Z_m \cap K_n$ for $m \leq j$ so we will have non-trivial trace only over $K_n$ and $Z_m \cap K_n$ for $m \leq j$. Like in the previous section, we find $Tr_{G_n/K_n}([A])$ and calculate the rest by using the fact that $Tr_{G_n/(Z_m \cap K_n)} = Tr_{K_n/(Z_m \cap K_n)} \circ Tr_{G_n/K_n}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} x & \epsilon\beta p^j \\ \beta p^j & x \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{ad - bc} \begin{pmatrix} adx - bcx - ab\beta p^j + cd\epsilon\beta p^j & d^2\epsilon\beta p^j - b^2\beta p^j \\ a^2\beta p^j - c^2\epsilon\beta p^j & adx - bcx + ab\beta p^j - cd\epsilon\beta p^j \end{pmatrix}$$

So we have the following conditions:

- $(d^2\epsilon - b^2)\beta p^j = (ad - bc)\epsilon\gamma p^j$
- $(a^2 - c^2\epsilon)\beta p^j = (ad - bc)\gamma p^j$
- $p^{n-j} | (ab - cd\epsilon)$

where $\gamma$ is any element in $(\mathbb{Z}/p^{n-j}\mathbb{Z})^\times$. Let us split this problem up into two cases:

### Case $p|a$

In this case we would know that $p$ does not divide either $b$ or $c$ and thus $b$ and $c$ would both be invertible. So the third bullet point can be rearranged as $a = \frac{cd\epsilon + lp^{n-j}}{b}$ for some $l \in \mathbb{Z}/p^j\mathbb{Z}$. Since $p|a$ and $p \not| c$, this equation tells us that $p|d$. Now we can plug this into the first bullet point and then the second bullet point:

$$\begin{aligned} & (d^2\epsilon - b^2)\beta p^j = (\tfrac{cd^2\epsilon}{b} - bc)\epsilon\gamma p^j \\ \iff \quad & (d^2\epsilon - b^2)\beta p^j = (d^2\epsilon - b^2)\tfrac{c}{b}\epsilon\gamma p^j \end{aligned}$$

Now we plug it into the second bullet point:

$$\begin{aligned} & (\tfrac{c^2d^2\epsilon^2}{b^2} - c^2\epsilon)\beta p^j = (\tfrac{cd^2\epsilon}{b} - bc)\gamma p^j \\ \iff \quad & (d^2\epsilon - b^2)\tfrac{c^2}{b^2}\epsilon\beta p^j = (d^2\epsilon - b^2)\tfrac{c}{b}\gamma p^j \end{aligned}$$

Since $p|d$, we know that $d^2\epsilon - b^2 \neq 0$, therefore, these equations tell us that $\beta p^j = \frac{c}{b}\epsilon\gamma p^j$ and $\frac{c^2}{b^2}\epsilon\beta p^j = \frac{c}{b}\gamma p^j$. This is only possible if $b \equiv c\epsilon \ (mod\ p^{n-j})$ and $\beta \equiv \gamma \ (mod\ p^{n-j})$ or if $b \equiv -c\epsilon \ (mod\ p^{n-j})$ and $\beta \equiv -\gamma \ (mod\ p^{n-j})$. In fact, all terms with $\gamma$ and $\beta$ are multiplied by $p^j$ so any matrix with $\beta \equiv \gamma \ (mod\ p^{n-j})$ is that same as having $\beta = \gamma$, and similar for $\beta = -\gamma$. Using the equation $a = \frac{cd\epsilon + lp^{n-j}}{b}$, we see now that we would have $a \equiv d \ (mod\ p^{n-j})$ and $b \equiv c\epsilon \ (mod\ p^{n-j})$ when $\beta = \gamma$ and we would have $a \equiv -d \ (mod\ p^{n-j})$ and $b \equiv -c\epsilon \ (mod\ p^{n-j})$ when $\beta = -\gamma$.

### Case $p \not| a$

In this case we would know that $a$ is invertible. So the third bullet point can be rearranged as $b = \frac{cd\epsilon + kp^{n-j}}{a}$ for some $k \in \mathbb{Z}/p^j\mathbb{Z}$. Now we can plug this into the first bullet point and then the second bullet point:

$$\begin{aligned} & (d^2\epsilon - \tfrac{c^2d^2\epsilon^2}{a^2})\beta p^j = (ad - \tfrac{c^2d\epsilon}{a})\epsilon\gamma p^j \\ \iff \quad & (a^2 - c^2\epsilon)\tfrac{d^2}{a^2}\epsilon\beta p^j = (a^2 - c^2\epsilon)\tfrac{d}{a}\epsilon\gamma p^j \end{aligned}$$

Now we can plug it into the second bullet point:

$$\begin{aligned} & (a^2 - c^2\epsilon)\beta p^j = (ad - \tfrac{c^2d\epsilon}{a})\gamma p^j \\ \iff \quad & (a^2 - c^2\epsilon)\beta p^j = (a^2 - c^2\epsilon)\tfrac{d}{a}\gamma p^j \end{aligned}$$

These equations are satisfied only if either $a^2 \equiv c^2\epsilon \ (mod\ p^{n-j})$ or $\frac{d^2}{a^2}\epsilon\beta p^j = \frac{d}{a}\epsilon\gamma p^j$ and $\beta p^j = \frac{d}{a}\gamma p^j$. The former condition would imply that $a \equiv c\sqrt{\epsilon} \ (mod\ p^{n-j})$, but this is impossible since $\epsilon$ is square-free by definition. The latter conditions are equivalent to $a \equiv d \ (mod\ p^{n-j})$ and $\beta = \gamma$ or if $a \equiv -d \ (mod\ p^{n-j})$ and $\beta = -\gamma$. Using the equation $b = \frac{cd\epsilon + kp^{n-j}}{a}$, we see now that we would have $b \equiv c\epsilon \ (mod\ p^{n-j})$ and $a \equiv d \ (mod\ p^{n-j})$ when $\beta = \gamma$ and we would have $b \equiv -c\epsilon \ (mod\ p^{n-j})$ and $a \equiv -d \ (mod\ p^{n-j})$ when $\beta = -\gamma$. These conditions agree with the previous case.

So we have either $X = \begin{pmatrix} a & \epsilon b + kp^{n-j} \\ b & a + lp^{n-j} \end{pmatrix}$ or $X = \begin{pmatrix} a & -\epsilon b + kp^{n-j} \\ b & -a + lp^{n-j} \end{pmatrix}$ where $k, l \in \mathbb{Z}/p^j\mathbb{Z}$. Now we find out how many of these matrices are distinct in $K_n \backslash G_n$:

$$\begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix}^{-1} \begin{pmatrix} a & \epsilon b + kp^{n-j} \\ b & a + lp^{n-j} \end{pmatrix} = \begin{pmatrix} 1 & k'p^{n-j} \\ 0 & 1 + l'p^{n-j} \end{pmatrix}$$

$$\begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix}^{-1} \begin{pmatrix} a & -\epsilon b + kp^{n-j} \\ b & -a + lp^{n-j} \end{pmatrix} = \begin{pmatrix} 1 & k'p^{n-j} \\ 0 & -1 + l'p^{n-j} \end{pmatrix}$$

Where $l = al' + k'b\epsilon$ and $k = \begin{cases} a^{-1}(bl + k'(a^2 - b^2\epsilon)) & \text{if } p \not| a \\ (b\epsilon)^{-1}(al - l'(a^2 - b^2\epsilon)) & \text{if } p|a \end{cases}$

Now we can compute the trace:

$$\begin{aligned}
Tr_{G_n/K_n}([A]_{G_n}) &= \sum_{\substack{X\in K_n\backslash G_n\\ X^{-1}AX\in K_n}} [X^{-1}AX]_{K_n}\\
&= \sum_{k,l}\left[\frac{1}{1+lp^{n-j}}\begin{pmatrix} x+xlp^{n-j} & \epsilon\beta p^j\\ \beta p^j & x+xlp^{n-j}\end{pmatrix}\right]_{K_n}\\
&\quad +\sum_{k,l}\left[\frac{1}{-1+lp^{n-j}}\begin{pmatrix} -x+xlp^{n-j} & \epsilon\beta p^j\\ \beta p^j & -x+xlp^{n-j}\end{pmatrix}\right]_{K_n}\\
&= \sum_{k,l}\left[\begin{pmatrix} x & \epsilon\beta p^j\\ \beta p^j & x\end{pmatrix}\right]_{K_n}+\sum_{k,l}\left[\begin{pmatrix} x & -\epsilon\beta p^j\\ -\beta p^j & x\end{pmatrix}\right]_{K_n}\\
&= p^{2j}\left[\begin{pmatrix} x & \epsilon\beta p^j\\ \beta p^j & x\end{pmatrix}\right]_{K_n}+p^{2j}\left[\begin{pmatrix} x & -\epsilon\beta p^j\\ -\beta p^j & x\end{pmatrix}\right]_{K_n}\\
&= p^{2j}\left[rj^j_{x,\beta}\right]_{K_n}+p^{2j}\left[rj^j_{x,-\beta}\right]_{K_n}
\end{aligned}$$

Now we can calculate the trace of $A$ over $Z_m\cap K_n$. Like the previous sections, we use our previous calculation to see that, for $A\in(Z_m\cap K_n)$, we always have $X^{-1}AX\in(Z_m\cap K_n)$ for any $X\in K_n$. We know $(Z_m\cap K_n)\backslash K_n = Z_m\backslash K_m$, so in $(Z_m\cap K_n)\backslash K_n$ we have:

$$\begin{pmatrix} a & b\\ \epsilon b & a\end{pmatrix}\sim\begin{cases}\begin{pmatrix} a' & 1\\ \epsilon & a'\end{pmatrix} & \text{if } p\not| b\\ \begin{pmatrix} 1 & pb'\\ pb' & 1\end{pmatrix} & \text{if } p|b\end{cases}$$

where $a'\in\mathbb{Z}/p^m\mathbb{Z}$ and $b'\in\mathbb{Z}/p^{m-1}\mathbb{Z}$ . So now we are ready to work out the trace:

$$\begin{aligned}
Tr_{G_n/(Z_m\cap K_n)}([rj^j_{x,\beta}]_{G_n}) &= \sum_{\substack{X\in(Z_m\cap K_n)\backslash K_n\\ X^{-1}AX\in(Z_m\cap K_n)}} p^{2j}[X^{-1}rj^j_{x,\beta}X]_{(Z_m\cap K_n)}\\
&\quad +\sum_{\substack{X\in(Z_m\cap K_n)\backslash K_n\\ X^{-1}AX\in(Z_m\cap K_n)}} p^{2j}[X^{-1}rj^j_{x,-\beta}X]_{(Z_m\cap K_n)}\\
&= \sum_a p^{2j}\left[\begin{pmatrix} x & \epsilon\beta p^j\\ \beta p^j & x\end{pmatrix}\right]_{(Z_m\cap K_n)}\\
&\quad +\sum_b p^{2j}\left[\begin{pmatrix} x & \epsilon\beta p^j\\ \beta p^j & x\end{pmatrix}\right]_{(Z_m\cap K_n)}\\
&\quad +\sum_a p^{2j}\left[\begin{pmatrix} x & -\epsilon\beta p^j\\ -\beta p^j & x\end{pmatrix}\right]_{(Z_m\cap K_n)}\\
&\quad +\sum_b p^{2j}\left[\begin{pmatrix} x & -\epsilon\beta p^j\\ -\beta p^j & x\end{pmatrix}\right]_{(Z_m\cap K_n)}\\
&= p^{m+2j}\left[rj^j_{x,\beta}\right]_{(Z_m\cap K_n)}+p^{m+2j-1}\left[rj^j_{x,\beta}\right]_{(Z_m\cap K_n)}\\
&\quad +p^{m+2j}\left[rj^j_{x,\beta}\right]_{(Z_m\cap K_n)}+p^{m+2j-1}\left[rj^j_{x,-\beta}\right]_{(Z_m\cap K_n)}\\
&= p^{m+2j-1}(p+1)\left(\left[rj^j_{x,\beta}\right]_{(Z_m\cap K_n)}+\left[rj^j_{x,-\beta}\right]_{(Z_m\cap K_n)}\right)
\end{aligned}$$

## Case $A=rt^i_{x,\alpha}$, $A=rk^i_{x,\alpha}$, $A=rci^{j,i}_{x,\alpha}$ and $A=rcj^{j,i}_{x,\alpha}$

These cases are grouped because they are in the same form, $A=\begin{pmatrix} x & p^i\epsilon_0\alpha\\ p^j\alpha & x\end{pmatrix}$ where $0\le j<i<n$ and $\epsilon_0$ is either $\epsilon$, a fixed square-free element, or 1. We will first do the cases $A=rt^i_{x,\alpha}$ and

$A = rk^i_{x,\alpha}$. We will also denote the groups $N_{t^i}$ and $N_{k^i}$ as:

$$N_A := \left\{ \begin{pmatrix} a & b\epsilon_0 p^i \\ b & a \end{pmatrix} : \begin{array}{c} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

where $i$ and $\epsilon_0$ are picked from the matrix $A$. For each matrix $A$ in this form, elements from $[A]_{G_n}$ are only contained in $N_A$, and no other group in $\mathcal{F}_n$, so we will have non-trivial trace only over $N_A$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} x & p^i\epsilon_0\alpha \\ \alpha & x \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{ad-bc} \begin{pmatrix} adx - bcx - ab\alpha + cd\epsilon_0 p^i\alpha & d^2\epsilon_0 p^i\alpha - b^2\alpha \\ a^2\alpha - c^2\epsilon_0 p^i\alpha & adx - bcx + ab\alpha - cd\epsilon_0 p^i\alpha \end{pmatrix}$$

To find the conditions on $X$ such that $A' \in N_A$, we need equate $A'$ to a generic term in $N_A$, i.e. $\begin{pmatrix} y & z\epsilon_0 p^i \\ z & y \end{pmatrix}$ where $y \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $z \in \mathbb{Z}/p^n\mathbb{Z}$. Now we have the following conditions:

- $a^2\alpha - c^2\epsilon_0 p^i\alpha = (ad-bc)z$
- $d^2\epsilon_0 p^i\alpha - b^2\alpha = (ad-bc)z\epsilon_0 p^i$
- $ab\alpha - cd\epsilon_0 p^i\alpha = 0$

It turns out that these conditions hold if and only if we have $b = \pm c\epsilon_0 p^i$ and $d = \pm a$. We are just stating this result now because we prove a more general result below.
This means that we need $X = \begin{pmatrix} a & b\epsilon_0 p^i \\ b & a \end{pmatrix}$ or $X = \begin{pmatrix} a & -b\epsilon_0 p^i \\ b & -a \end{pmatrix}$
Now we need to find how many of these elements are distinct in $N_A \backslash G_n$:

$$\begin{pmatrix} x & \epsilon_0 y p^i \\ y & x \end{pmatrix} \begin{pmatrix} a & b\epsilon_0 p^i \\ b & a \end{pmatrix} = \begin{pmatrix} b\epsilon_0 y p^i + ax & (ayp^j + bx)\epsilon_0 p^i \\ ayp^j + bx & b\epsilon_0 y p^i + ax \end{pmatrix}$$

$$\begin{pmatrix} x & \epsilon_0 y p^i \\ y & x \end{pmatrix} \begin{pmatrix} a & -b\epsilon_0 p^i \\ b & -a \end{pmatrix} = \begin{pmatrix} b\epsilon_0 y p^i + ax & -(ayp^j + bx)\epsilon_0 p^i \\ ayp^j + bx & -(b\epsilon_0 y p^i + ax) \end{pmatrix}$$

By choosing $x = a^{-1}(1 - b\epsilon_0 y p^i)$ and $y = -b(a^2 - b^2\epsilon_0 p^{i-j})^{-1}$ we get the following:

$$\begin{pmatrix} x & \epsilon_0 y p^i \\ y & x \end{pmatrix} \begin{pmatrix} a & b\epsilon_0 p^i \\ b & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} x & \epsilon_0 y p^i \\ y & x \end{pmatrix} \begin{pmatrix} a & -b\epsilon_0 p^i \\ b & -a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Now we can easily calculate the trace:

$$\begin{aligned} Tr_{G_n/N_A}([A]_{G_n}) &= \sum_{\substack{X \in N_A \backslash G_n \\ X^{-1}AX \in N_A}} [X^{-1}AX]_{N_A} \\ &= \left[ \begin{pmatrix} x & \epsilon_0\alpha p^i \\ p^j\alpha & x \end{pmatrix} \right]_{N_A} + \left[ \begin{pmatrix} x & -\epsilon_0\alpha p^i \\ -p^j\alpha & x \end{pmatrix} \right]_{N_A} \end{aligned}$$

Now we will do the cases $A = rci^{j,i}_{x,\alpha}$ and $A = rcj^{j,i}_{x,\alpha}$. When $A = rci^{j,i}_{x,\alpha}$, $A$ is only contained in $N_{t^{i-j}}$ and $Z_m \cap N_{t^{i-j}}$ for $m \leq j$. When $A = rcj^{j,i}_{x,\alpha}$, $A$ is only contained in $N_{k^{i-j}}$ and $Z_m \cap N_{k^{i-j}}$ for $m \leq j$. Now we will redefine $N_A$ as:

$$N_A := \left\{ \begin{pmatrix} a & b\epsilon_0 p^{i-j} \\ b & a \end{pmatrix} : \begin{array}{c} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

where $i$,$j$ and $\epsilon_0$ are picked from the matrix $A$. For each matrix $A$ in this form, elements from $[A]_{G_n}$ are only contained in $N_A$ and $Z_m \cap N_A$ for $m \leq j$, and no other group. Like in the previous section, we find $Tr_{G_n/N_A}([A])$ and calculate the rest by using the fact that $Tr_{G_n/(Z_m \cap N_A)} = Tr_{N_A/(Z_m \cap N_A)} \circ Tr_{G_n/N_A}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} x & p^i\epsilon_0\alpha \\ p^j\alpha & x \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \frac{1}{ad-bc} \begin{pmatrix} adx - bcx - abp^j\alpha + cd\epsilon_0 p^i\alpha & d^2\epsilon_0 p^i\alpha - b^2 p^j\alpha \\ a^2p^j\alpha - c^2\epsilon_0 p^i\alpha & adx - bcx + abp^j\alpha - cd\epsilon_0 p^i\alpha \end{pmatrix}$$

To find the conditions on $X$ such that $A' \in N_A$, we need equate $A'$ to a generic term in $N_A$, i.e. $\begin{pmatrix} y & z'\epsilon_0 p^{i-j} \\ z' & y \end{pmatrix}$ where $y \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $z' \in \mathbb{Z}/p^n\mathbb{Z}$. Now we have the following conditions:

- $a^2p^j\alpha - c^2\epsilon_0 p^i\alpha = (ad-bc)z'$
- $d^2\epsilon_0 p^i\alpha - b^2p^j\alpha = (ad-bc)z'\epsilon_0 p^{i-j}$
- $abp^j\alpha - cd\epsilon_0 p^i\alpha = 0$

We know that $p$ cannot divide $ad-bc$ because $X$ is invertible, and we also know that $i$ is strictly greater than $j$ so the first bullet point implies that we have $p^j|z'$. Without loss of generality, we can replace $z'$ with $p^jz$ and plug this into the three conditions:

- $a^2p^j\alpha - c^2\epsilon_0 p^i\alpha = (ad-bc)zp^j$
- $d^2\epsilon_0 p^i\alpha - b^2p^j\alpha = (ad-bc)z\epsilon_0 p^i$
- $abp^j\alpha - cd\epsilon_0 p^i\alpha = 0$

Since $i$ is strictly greater than $j$, the second bullet point implies $p|b$, therefore $a$ and $d$ are invertible. Using this, we can rearrange the third bullet point to obtain $b = \frac{cd\epsilon_0 p^{i-j}\alpha - kp^{n-j}}{a\alpha}$ where $k \in \mathbb{Z}/p^j\mathbb{Z}$. Plugging this into the first bullet point gives us the following:

$$\begin{aligned} & a^2p^j\alpha - c^2\epsilon_0 p^i\alpha = adzp^j - \tfrac{c^2dz\epsilon_0 p^i\alpha}{a\alpha} \\ \iff \quad & p^j\alpha(a^2 - c^2\epsilon_0 p^{i-j}) = \tfrac{d}{a}zp^j(a^2 - c^2\epsilon_0 p^{i-j}) \end{aligned}$$

But $a^2 \neq c^2\epsilon_0 p^{i-j}$ because $p \not| a$ therefore $p^j\alpha = \frac{d}{a}zp^j$ thus $a\alpha \equiv dz \ (mod\ p^{n-j})$.
Plugging the expression for $b$ into the second bullet point gives us the following:

$$\begin{aligned} & d^2\epsilon_0 p^i\alpha - \tfrac{c^2d^2\epsilon_0^2 p^{2i-j}\alpha}{a^2} = adzp^i - \tfrac{c^2dz\epsilon_0 p^{2i-j}\epsilon_0}{a} \\ \iff \quad & \tfrac{d^2}{a^2}\epsilon_0 p^i\alpha(a^2 - c^2\epsilon_0 p^{i-j}) = \tfrac{d}{a}z\epsilon_0 p^i(a^2 - c^2\epsilon_0 p^{i-j}) \end{aligned}$$

Since $a^2 \neq c^2\epsilon_0 p^{i-j}$ we get $\frac{d^2}{a^2}\epsilon_0 p^i\alpha = \frac{d}{a}z\epsilon_0 p^i$. Now we can plug in $a\alpha \equiv dz \ (mod\ p^{n-j})$ which gives us $z^2 \equiv \alpha^2 \ (mod\ p^{n-i})$. But if we look back at the equation $p^j\alpha = \frac{d}{a}zp^j$, we see that we must use the weaker condition $z^2 \equiv \alpha^2 \ (mod\ p^{n-j})$. So we now get $X = \begin{pmatrix} a & b\delta\epsilon_0 p^{i-j} + kp^{n-j} \\ b & a\delta + lp^{n-j} \end{pmatrix}$ where $\delta^2 \equiv 1^2 \ (mod\ p^{n-j})$:

$$\begin{pmatrix} a & b\delta\epsilon_0 p^{i-j} + kp^{n-j} \\ b & a\delta + lp^{n-j} \end{pmatrix}^{-1} \begin{pmatrix} x & p^i\epsilon_0\alpha \\ p^j\alpha & x \end{pmatrix} \begin{pmatrix} a & b\delta\epsilon_0 p^{i-j} + kp^{n-j} \\ b & a\delta + lp^{n-j} \end{pmatrix}$$

$$= \begin{pmatrix} x+0 & \frac{a^2\epsilon_0\alpha p^i - b^2\epsilon_0^2 p^{2i-j}\alpha}{a^2\delta - b^2\delta\epsilon_0 p^{i-j} + p^{n-j}(al-bk)} \\ \frac{a^2p^j\alpha - b^2\epsilon_0 p^i\alpha}{a^2\delta - b^2\delta\epsilon_0 p^{i-j} + p^{n-j}(al-bk)} & x-0 \end{pmatrix}$$

$$= \begin{pmatrix} x & \delta p^i \epsilon_0 \alpha \\ \delta p^j \alpha & x \end{pmatrix}$$

Finally, we find out how many of theses matrices are distinct in $N_A \backslash G_n$:

$$\begin{pmatrix} x & \epsilon_0 y p^{i-j} \\ y & x \end{pmatrix} \begin{pmatrix} a & b\delta\epsilon_0 p^{i-j} + kp^{n-j} \\ b & a\delta + lp^{n-j} \end{pmatrix}$$

$$= \begin{pmatrix} b\epsilon_0 y p^{i-j} + ax & (ay+bx)\delta\epsilon_0 p^{i-j} + k' p^{n-j} \\ ay + bx & (b\epsilon_0 y p^{i-j} + ax)\delta + l' p^{n-j} \end{pmatrix}$$

Where $k' = xk + \epsilon_0 y l p^{i-j}$ and $l' = yk + xl$. By choosing $x = a^{-1}(1 - b\epsilon_0 y p^i)$ and $y = -b(a^2 - b^2\epsilon_0 p^i)^{-1}$ we get the following:

$$\begin{pmatrix} x & \epsilon_0 y p^i \\ y p^j & x \end{pmatrix} \begin{pmatrix} a & b\delta\epsilon_0 p^{i-j} + kp^{n-j} \\ b & a\delta + lp^{n-j} \end{pmatrix} = \begin{pmatrix} 1 & k' p^{n-j} \\ 0 & \delta + l' p^{n-j} \end{pmatrix}$$

so we effectively have $p^j$ choices for $k'$, $l'$ and 2 choices[1]for $\delta$. Now we can calculate the trace:

$$\begin{aligned} Tr_{G_n/N_A}([A]_{G_n}) &= \sum_{\substack{X \in N_A \backslash G_n \\ X^{-1}AX \in N_A}} [X^{-1}AX]_{N_A} \\ &= p^{2j} \left( \left[ \begin{pmatrix} x & \epsilon_0 \alpha p^i \\ p^j \alpha & x \end{pmatrix} \right]_{N_A} + \left[ \begin{pmatrix} x & -\epsilon_0 \alpha p^i \\ -p^j \alpha & x \end{pmatrix} \right]_{N_A} \right) \end{aligned}$$

Now we calculate the trace of $A$ over $Z_m \cap N_A$. Like the previous sections, we use our previous calculation to see that, for $A \in (Z_m \cap N_A)$, we always have $X^{-1}AX \in (Z_m \cap N_A)$ for any $X \in N_A$. We know $(Z_m \cap N_A)\backslash N_A = Z_m \backslash N_A^{(m)}$, so in $(Z_m \cap N_A)\backslash N_A$ we have $\left[ \begin{pmatrix} a & p^{i-j}\epsilon_0 b \\ b & a \end{pmatrix} \right] = \left[ \begin{pmatrix} 1 & p^{i-j}\epsilon_0 b' \\ b' & 1 \end{pmatrix} \right]$ where $b' \in \mathbb{Z}/p^m\mathbb{Z}$. So now we are ready to work out the trace:

$$\begin{aligned} Tr_{G_n/(Z_m \cap N_A)}([A]_{G_n}) = & \sum_{b'} p^{2j} \left[ \begin{pmatrix} x & \epsilon_0 \alpha p^i \\ p^j \alpha & x \end{pmatrix} \right]_{(Z_m \cap N_A)} \\ & + \sum_{b'} p^{2j} \left[ \begin{pmatrix} x & -\epsilon_0 \alpha p^i \\ -p^j \alpha & x \end{pmatrix} \right]_{(Z_m \cap N_A)} \\ = & \; p^{2j+m} \left( \left[ \begin{pmatrix} x & \epsilon_0 \alpha p^i \\ p^j \alpha & x \end{pmatrix} \right]_{(Z_m \cap N_A)} + \left[ \begin{pmatrix} x & -\epsilon_0 \alpha p^i \\ -p^j \alpha & x \end{pmatrix} \right]_{(Z_m \cap N_A)} \right) \end{aligned}$$

[1]Although our calculations show that $\delta^2 \equiv 1^2 \; (mod \; p^{n-j})$, the terms $kp^{n-j}$ and $lp^{n-j}$ make it so that we can treat $\delta$ as if it is equal to $\pm 1$.

# Chapter 5

# Constructing map $\mathcal{L}$

In this chapter, we will construct a map $\mathcal{L}$ which makes the diagram below (diagram (1) from chapter 2.6.2) commute for general $n$:

$$\begin{array}{ccccccc} ker(Log) & \to & K_1(\mathbb{Z}_p[G_n]) & \xrightarrow{Log} & \mathbb{Z}_p[Conj(G_n)] & \to & coker(Log) \\ & & \downarrow \theta_n & & \downarrow \psi_n & & \\ ker(\mathcal{L}) & \dashrightarrow & \prod_{U\in\mathcal{F}_n}\Lambda(U^{ab})^\times & \overset{\mathcal{L}}{\dashrightarrow} & \mathbb{Q}_p\otimes_{\mathbb{Z}_p}\prod_{U\in\mathcal{F}_n}\mathbb{Z}_p[U^{ab}] & \dashrightarrow & coker(\mathcal{L}) \end{array}$$

where $\mathcal{F}_n = \{Z_n, C_n, T_n, K_n, N_{t^i}, N_{k^i} | \forall i = 1, 2, ..., n-1\}$. We will then find $\Theta_{n,\mathbb{Z}_p}$ (Definition 5.1), a subgroup of $\prod_{U\in\mathcal{F}_n}\Lambda(U^{ab})^\times$ which, under the map $\mathcal{L}$, contains $\Psi_{n,\mathbb{Z}_p}$ (defined in Theorem 4.2). The group $\Theta_{n,\mathbb{Z}_p}$ contains the image of $\theta_n$. Recall the definition of $\psi_n$:

**Definition 2.9** *For $U \in \mathcal{F}_n$, let $Tr_{G_n/U}$ be the map:*

$$\begin{array}{ccc} \mathbb{Z}_p[Conj(G_n)] & \to & \mathbb{Z}_p[Conj(U)] \\ [A]_{G_n} & \mapsto & \sum_{\substack{X\in U\backslash G_n \\ X^{-1}AX\in U}} [X^{-1}AX]_U \end{array}$$

*and let $proj_U$ be the natural projection from $\mathbb{Z}_p[Conj(U)]$ to $\mathbb{Z}_p[Conj(U^{ab})] = \mathbb{Z}_p[U^{ab}]$, then:*

$$\begin{array}{ccc} \psi_n : \mathbb{Z}_p[Conj(G_n)] & \to & \prod_{U\in\mathcal{F}_n}\mathbb{Z}_p[U^{ab}] \\ \psi_n : [A]_{G_n} & \mapsto & \prod_{U\in\mathcal{F}_n} proj_U \circ Tr_{G_n/U}([A]_{G_n}) \end{array}$$

For each individual subgroup, we use this notation: $\psi_U := proj_U \circ Tr_{\mathcal{G}/U}([A]_{\mathcal{G}})$. This means we can write $\psi_n = \prod_{U\in\mathcal{F}_n}\psi_U$.

We will use notation from chapter 4 for the conjugacy classes of $GL_2(\mathbb{Z}/p^n\mathbb{Z})$:

| $i_x$ | $c^0_{x,1}$ | $t^0_{w,y}$ | $k^0_{z,y}$ | $rt^i_{x,\alpha}$ | $rk^i_{x,\alpha}$ |
|---|---|---|---|---|---|
| $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ | $\begin{pmatrix} x & 0 \\ 1 & x \end{pmatrix}$ | $\begin{pmatrix} w+y & 0 \\ 0 & w-y \end{pmatrix}$ | $\begin{pmatrix} z & \epsilon y \\ y & z \end{pmatrix}$ | $\begin{pmatrix} x & p^i\alpha \\ \alpha & x \end{pmatrix}$ | $\begin{pmatrix} x & p^i\epsilon\alpha \\ \alpha & x \end{pmatrix}$ |

| $rc^j_{x,1}$ | $rci^{j,i}_{x,\alpha}$ | $rcj^{j,i}_{x,\alpha}$ | $ri^j_{x,\beta}$ | $rj^j_{x,\beta}$ |
|---|---|---|---|---|
| $\begin{pmatrix} x & 0 \\ p^j & x \end{pmatrix}$ | $\begin{pmatrix} x & p^i\alpha \\ p^j\alpha & x \end{pmatrix}$ | $\begin{pmatrix} x & p^i\epsilon\alpha \\ p^j\alpha & x \end{pmatrix}$ | $\begin{pmatrix} x+\beta p^j & 0 \\ 0 & x-\beta p^j \end{pmatrix}$ | $\begin{pmatrix} x & p^j\epsilon\beta \\ p^j\beta & x \end{pmatrix}$ |

$$i, j = 1, 2, ..., n-1 \text{ s.t } j < i,\ x, y \in (\mathbb{Z}/p^n\mathbb{Z})^\times \text{ and } w, z \in \mathbb{Z}/p^n\mathbb{Z} \text{ s.t } y \not\equiv \pm w\ (mod\ p)$$

$$\alpha \in (\mathbb{Z}/p^{n-i}\mathbb{Z})^\times \text{ and } \beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times$$

where $\epsilon$ is a fixed non-square element in $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Recall that $c^0_{x,y} := \begin{pmatrix} x & 0 \\ y & x \end{pmatrix}$ and $rc^j_{x,\beta} := \begin{pmatrix} x & 0 \\ \beta p^j & x \end{pmatrix}$.
As explained in chapter 2.6.2, we will find $\mathcal{L}$ using the following diagram ([14], Proof of Theorem 6.8):

$$\begin{array}{ccccc} K_1(\mathbb{Z}_p[G_n]) & \xrightarrow{log} & \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[Conj(G_n)] & \xrightarrow{1-\frac{\varphi}{p}} & \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[Conj(G_n)] \\ \downarrow \theta & \circlearrowleft & \downarrow \psi_n & & \downarrow \psi_n \\ \prod_{U\in\mathcal{F}_n} \mathbb{Z}_p[U^{ab}]^\times & \xrightarrow{log} & \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \prod_{U\in\mathcal{F}_n} \mathbb{Z}_p[U^{ab}] & \overset{f}{\dashrightarrow} & \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \prod_{U\in\mathcal{F}_n} \mathbb{Z}_p[U^{ab}] \end{array}$$

Where $\varphi$ is the endomorphism on $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[Conj(G_n)]$, defined in the following way:

$$\varphi : \sum a_g g \mapsto \sum a_g g^p$$

In the above diagram, the left square is commutative, so we just need to find a map $f$ such that the right square commutes and then we can just set $\mathcal{L} = f \circ log$.

## 5.1 The explicit construction of the map $f$

Recall $\mathcal{F}_n = \{Z_n, C_n, T_n, K_n, N_{t^i}, N_{k^i} | \forall i = 1, 2, ..., n-1\}$ where these subgroups are defined as follows:

$$Z_n := \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\}$$

$$C_n := \left\{ \begin{pmatrix} a & 0 \\ c & a \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ c \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

$$T_n := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\}$$

$$K_n := \left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} : \begin{array}{l} a, b \in \mathbb{Z}/p^n\mathbb{Z} \\ \text{s.t. } p \not| (a^2 - \epsilon b^2) \end{array} \right\}$$

$$N_{t^i} := \left\{ \begin{pmatrix} a & bp^i \\ b & a \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

$$N_{k^i} := \left\{ \begin{pmatrix} a & b\epsilon p^i \\ b & a \end{pmatrix} : \begin{array}{l} a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \\ b \in \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\}$$

**Proposition 5.1** *$f := \prod_{U\in\mathcal{F}_n} f_U$ such that:*

$$f_U((a_V)) := \begin{cases} a_U - p\varphi(a_U) - \frac{1}{p}\varphi\left(T_U(a_U)\right) + p\varphi\left(T_U(a_U)\right) - [G_n : U]\lambda_f((a_V)) \\ \quad - \sum\limits_{\substack{N=N_{t^l},N_{k^l} \\ l\le i}} \mu_{f,N}(a_N) \sum\limits_\beta rc^{n-l}_{1,\beta} + \mu_{f,U}(a_U) \sum\limits_\beta rc^{n-i}_{1,\beta} + \nu_{f,U}(a_{C_n}) & \text{if } U = N_{t^i} \text{ or } N_{k^i} \\ a_{C_n} - \varphi(a_{C_n}) - \frac{1}{p}\varphi\left(T_{C_n}(a_{C_n})\right) - \sum\limits_{N=N_{t^l},N_{k^l}} \mu_{f,N}(a_N) \sum\limits_\beta rc^{n-l}_{1,\beta} \\ \quad + T_{C_n}(\varphi(a_{C_n})) - [G_n : C_n]\lambda_f((a_V)) & \text{if } U = C_n \\ a_{Z_n} - \frac{\varphi(a_{Z_n})}{p} - [G_n : Z_n]\lambda_f((a_V)) & \text{if } U = Z_n \\ a_U - \frac{\varphi(a_U)}{p} + \frac{1}{p}\Big(T_U(\varphi(a_U)) - \varphi(T_U(a_U))\Big) - [G_n : U]\lambda_f((a_V)) & \text{otherwise} \end{cases}$$

*where* $\sum_\beta$ *is a sum of all* $\beta \in (\mathbb{Z}/p^l\mathbb{Z})^\times$, $T_U(a_U) = \frac{Tr_{U/Z_n}(a_U)}{[U:Z_n]}$, $\lambda_f$ *is a map from* $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \prod_{U\in\mathcal{F}_n} \mathbb{Z}_p[U]$ *to* $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[Z_n]$, $\mu_{f,N}$ *is a map from* $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[N]$ *to* $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[Z_{n-i} \cap C_n]$ *and* $\nu_{f,N}$ *is a map from* $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[C_n]$ *to* $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[N]$ *for* $N \in \{N_{t^i}, N_{k^i} | i = 1, 2, ..., n-1\}$. *These maps are defined*[1] *in the following way:*

$$\lambda_f((a_V)) = \frac{1}{p} \sum_{W=C_n,T_n,K_n} \frac{Tr_{W/Z_n}\left(\varphi\left(a_W - T_W(a_W)\right)\right)}{[W : Z_n]}$$

$$\mu_{f,N}(a_N) = \frac{p}{2}\varphi\left(\frac{Tr_{N/(Z_{n-i-1}\cap N)}(a_N)}{[N : Z_{n-i-1} \cap N]} - \frac{Tr_{N/(Z_{n-i}\cap N)}(a_N)}{[N : Z_{n-i} \cap N]}\right)$$

$$\nu_{f,N}(a_{C_n}) = Tr_{C_n/(Z_{n-i}\cap C_n)}\Big(a_{C_n} - \varphi(a_{C_n}) - T_{C_n}(a_{C_n}) + T_{C_n}(\varphi(a_{C_n}))\Big)$$

*Note that* $Z_n$ *is a subgroup of any* $U \in \mathcal{F}_n$, *so any element* $a_{Z_n} \in \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[Z_n]$ *can also be thought as an element of* $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[U]$. *In particular, for any* $U \in \mathcal{F}_n$, *we have* $\lambda_f((a_V)) \in \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[U]$. *Also note that* $Z_{n-i} \cap C_n = Z_{n-i} \cap N$ *for* $N \in \{N_{t^i}, N_{k^i} | i = 1, 2, ..., n-1\}$ *so we have both* $\mu_{f,N} \in \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[Z_{n-i} \cap C_n]$ *and* $\mu_{f,N} \in \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[Z_{n-i} \cap N]$.

**Proof:**

We will verify that this map $f$ makes the diagram commute by calculating $\psi_n \circ (1 - \frac{\varphi}{p})$ and $f \circ \psi_n$ of each conjugacy class[2] of $G_n$. In the previous chapter we calculated $\psi_n(A)$ for each matrix representation of each conjugacy class of $G_n$ (Table 3). We will use this information to help us calculate both $\psi_n \circ (1 - \frac{\varphi}{p})$ and $f \circ \psi_n$.

In the following tables we will use a condensed notion to save space when writing elements in $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \prod_{U\in\mathcal{F}_n} \mathbb{Z}_p[U]$:

$$\text{Let } (a_1, a_2, ..., a_m) \in A_1 \times A_2 \times ... \times A_m$$

We will write $(a_k, a_l)_{A_k,A_l}$ to indicate that all entries are zero except for $a_k \in A_k$ and $a_l \in A_l$. We will also write $(a_i, a(U))_{A_i,A_{n_1}\times A_{n_2}\times ...A_{n_{i-1}}\times A_{n_m}}$ if the $A_i^{th}$ entry is $a_i$ and the other entries, $U \in A_{n_1} \times A_{n_2} \times ...A_{n_{i-1}} \times A_{n_{i-1}} ... \times A_{n_m}$, can be expressed as a function $a(U)$.

[1] For more details on the trace maps used in $\lambda_f, \mu_{f,N}$ and $\nu_{f,N}$, please refer to Chapter 4, before the proof of Theorem 4.1, where we discuss $Tr_{U/(Z_m\cap U)}$ for different values of $m$ and groups $U$.

[2] Since all maps $f$, $\psi_n$ and $\varphi$ act on $\mathbb{Q}_p$ exactly like the identity map, we only need to calculate $\psi_n \circ (1 - \frac{\varphi}{p})$ and $f \circ \psi_n$ of each element in $Conj(G_n)$ rather than the whole of $\mathbb{Q}_p \otimes \mathbb{Z}_p[Conj(G_n)]$.

| $A$ | $(1-\frac{\varphi}{p})(A)$ | $(\psi_n \circ (1-\frac{\varphi}{p}))(A)$ |
|---|---|---|
| $i_x$ | $i_x - \frac{i_{x^p}}{p}$ | $([G_n : U](i_x - i_{x^p}/p))_{\mathcal{F}_n}$ |
| $c^0_{x,1}$ | $c^0_{x,1} - \frac{rc^1_{x^p,x^{p-1}}}{p}$ | $\left(\sum_{y\in(\mathbb{Z}/p^n\mathbb{Z})^\times} c^0_{x,y} - p\sum_{\beta\in(\mathbb{Z}/p^{n-1}\mathbb{Z})^\times} rc^1_{x^p,\beta}\right)_{C_n}$ |
| $t^0_{w,y}$ | $t^0_{w,y} - \frac{(t^0_{w,y})^p}{p}$ | $\left(t^0_{w,y} + t^0_{w,-y} - \frac{\psi_n((t^0_{w,y})^p)}{p}\right)_{T_n}$ |
| $k^0_{z,y}$ | $k^0_{z,y} - \frac{(k^0_{z,y})^p}{p}$ | $\left(k^0_{z,y} + k^0_{z,-y} - \frac{\psi_n((k^0_{z,y})^p)}{p}\right)_{K_n}$ |
| $rt^i_{x,\alpha}$ for $i < n-1$ | $rt^i_{x,\alpha} - \frac{(rt^i_{x,\alpha})^p}{p}$ | $\left(rt^i_{x,\alpha} + rt^i_{x,-\alpha} - \frac{\psi_n((rt^i_{x,\alpha})^p)}{p}\right)_{N_{t^i}}$ |
| $rt^{n-1}_{x,\alpha}$ | $rt^{n-1}_{x,\alpha} - \frac{rc^1_{x^p,\alpha x^{p-1}}}{p}$ | $\left(rt^{n-1}_{x,\alpha} + rt^{n-1}_{x,-\alpha} - p\sum_{\beta\in(\mathbb{Z}/p^{n-1}\mathbb{Z})^\times} rc^1_{x^p,\beta}, -p\sum_{\beta\in(\mathbb{Z}/p^{n-1}\mathbb{Z})^\times} rc^1_{x^p,\beta}\right)_{N_{t^{n-1}},C_n\times N_{k^{n-1}}}$ |
| $rk^i_{x,\alpha}$ for $i < n-1$ | $rk^i_{x,\alpha} - \frac{(rk^i_{x,\alpha})^p}{p}$ | $\left(rk^i_{x,\alpha} + rk^i_{x,-\alpha} - \frac{\psi_n((rk^i_{x,\alpha})^p)}{p}\right)_{N_{k^i}}$ |
| $rk^{n-1}_{x,\alpha}$ | $rk^{n-1}_{x,\alpha} - \frac{rc^1_{x^p,\alpha x^{p-1}}}{p}$ | $\left(rk^{n-1}_{x,\alpha} + rk^{n-1}_{x,-\alpha} - p\sum_{\beta\in(\mathbb{Z}/p^{n-1}\mathbb{Z})^\times} rc^1_{x^p,\beta}, -p\sum_{\beta\in(\mathbb{Z}/p^{n-1}\mathbb{Z})^\times} rc^1_{x^p,\beta}\right)_{N_{k^{n-1}},C_n\times N_{t^{n-1}}}$ |
| $rc^j_{x,1}$ for $j < n-1$ | $rc^j_{x,1} - \frac{rc^{j+1}_{x^p,x^{p-1}}}{p}$ | $\left(p^{2j}\sum_{\beta\in(\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} rc^j_{x,\beta} - p^{2j+1}\sum_{\beta\in(\mathbb{Z}/p^{n-j-1}\mathbb{Z})^\times} rc^{j+1}_{x^p,\beta} - p^{2j+1}\sum_{\beta\in(\mathbb{Z}/p^{n-j-1}\mathbb{Z})^\times} rc^{j+1}_{x^p,\beta}\right)_{C_n\times\prod_{i=n-j}^{n-1}(N_{t^i}\times N_{k^i}),N_{t^{n-j-1}}\times N_{k^{n-j-1}}}$ |
| $rc^{n-1}_{x,1}$ | $rc^{n-1}_{x,1} - \frac{i_{x^p}}{p}$ | $\left(p^{2n-2}\sum_{\beta\in(\mathbb{Z}/p\mathbb{Z})^\times} rc^{n-1}_{x,\beta} - \frac{[G_n:C_n]}{p}i_{x^p}, -\frac{[G_n:U]}{p}i_{x^p}\right)_{C_n\times\prod_{i=1}^{n-1}(N_{t^i}\times N_{k^i}),\mathcal{F}_n\setminus(C_n\times\prod_{i=1}^{n-1}(N_{t^i}\times N_{k^i}))}$ |
| $rci^{j,i}_{x,\alpha}$ for $i < n-1$ | $rci^{j,i}_{x,\alpha} - \frac{(rci^{j,i}_{x,\alpha})^p}{p}$ | $\left(p^{2j}(rci^{j,i}_{x,\alpha} + rci^{j,i}_{x,-\alpha}) - \frac{\psi_n((rci^{j,i}_{x,\alpha})^p)}{p}\right)_{N_{t^{i-j}}}$ |
| $rci^{j,n-1}_{x,\alpha}$ | $rci^{j,n-1}_{x,\alpha} - \frac{rc^{j+1}_{x^p,\alpha x^{p-1}}}{p}$ | $\left(p^{2j}(rci^{j,n-1}_{x,\alpha} + rci^{j,n-1}_{x,-\alpha}) - p^{2j+1}\sum_{\beta\in(\mathbb{Z}/p^{n-j-1}\mathbb{Z})^\times} rc^{j+1}_{x^p,\beta}, -p^{2j+1}\sum_{\beta\in(\mathbb{Z}/p^{n-j-1}\mathbb{Z})^\times} rc^{j+1}_{x^p,\beta}\right)_{N_{t^{n-1-j}},C_n\times N_{k^{n-1-j}}\times\prod_{i=n-j}^{n-1}(N_{t^i}\times N_{k^i})}$ |
| $rcj^{j,i}_{x,\alpha}$ for $i < n-1$ | $rcj^{j,i}_{x,\alpha} - \frac{(rcj^{j,i}_{x,\alpha})^p}{p}$ | $\left(p^{2j}(rcj^{j,i}_{x,\alpha} + rcj^{j,i}_{x,-\alpha}) - \frac{\psi_n((rcj^{j,i}_{x,\alpha})^p)}{p}\right)_{N_{k^{i-j}}}$ |
| $rcj^{j,n-1}_{x,\alpha}$ | $rcj^{j,n-1}_{x,\alpha} - \frac{rc^{j+1}_{x^p,\alpha x^{p-1}}}{p}$ | $\left(p^{2j}(rcj^{j,i}_{x,\alpha} + rcj^{j,i}_{x,-\alpha})) - p^{2j+1}\sum_{\beta\in(\mathbb{Z}/p^{n-j-1}\mathbb{Z})^\times} rc^{j+1}_{x^p,\beta}, -p^{2j+1}\sum_{\beta\in(\mathbb{Z}/p^{n-j-1}\mathbb{Z})^\times} rc^{j+1}_{x^p,\beta}\right)_{N_{k^{n-1-j}},C_n\times N_{t^{n-1-j}}\times\prod_{i=n-j}^{n-1}(N_{t^i}\times N_{k^i})}$ |
| $ri^j_{x,\beta}$ for $j < n-1$ | $ri^j_{x,\beta} - \frac{(ri^j_{x,\beta})^p}{p}$ | $\left(p^{2j}(ri^j_{x,\beta} + ri^j_{x,-\beta}) - \frac{\psi_n((ri^j_{x,\beta})^p)}{p}\right)_{T_n}$ |
| $ri^{n-1}_{x,\beta}$ | $ri^{n-1}_{x,\beta} - \frac{i_{x^p}}{p}$ | $\left(p^{2n-2}(ri^{n-1}_{x,\beta} + ri^{n-1}_{x,-\beta}) - \frac{[G_n:T_n]}{p}i_{x^p}, -\frac{[G_n:U]}{p}i_{x^p}\right)_{T_n,\mathcal{F}_n\setminus T_n}$ |
| $rj^j_{x,\beta}$ for $j < n-1$ | $rj^j_{x,\beta} - \frac{(rj^j_{x,\beta})^p}{p}$ | $\left(p^{2j}(rj^j_{x,\beta} + rj^j_{x,-\beta}) - \frac{\psi_n((rj^j_{x,\beta})^p)}{p}\right)_{K_n}$ |
| $rj^{n-1}_{x,\beta}$ | $rj^{n-1}_{x,\beta} - \frac{i_{x^p}}{p}$ | $\left(p^{2n-2}(rj^{n-1}_{x,\beta} + rj^{n-1}_{x,-\beta}) - \frac{[G_n:K_n]}{p}i_{x^p}, -\frac{[G_n:U]}{p}i_{x^p}\right)_{K_n,\mathcal{F}_n\setminus K_n}$ |

Where $i,j = 1,2,...,n-1$ s.t $j<i$, $x,y \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $w,z \in \mathbb{Z}/p^n\mathbb{Z}$ s.t $y \not\equiv \pm w \ (mod\ p)$.
Also $k,l \in \mathbb{Z}/p^j\mathbb{Z}, \alpha \in (\mathbb{Z}/p^{n-i}\mathbb{Z})^\times$ and $\beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times$.

There was not enough space on the table to explicitly write out $\varphi(t^0_{w,y})$, $\varphi(k^0_{z,y})$, $\varphi(rt^i_{x,\alpha})$,

$\varphi(rk^i_{x,\alpha})$, $\varphi(rci^{j,i}_{x,\alpha})$, $\varphi(rcj^{j,i}_{x,\alpha})$, $\varphi(ri^j_{x,\beta})$ and $\varphi(rj^j_{x,\beta})$. So we will describe them explicitly now: $(t^0_{w,y})^p = t^0_{w',y'}$ where

$$w' = \sum_{\substack{0\le h\le p\\ 2|h}} \binom{p}{h} w^{p-h}y^h$$

and

$$y' = \sum_{\substack{0\le h\le p\\ 2|h}} \binom{p}{h} w^{p-h}y^h$$

$(k^0_{z,y})^p = k^0_{z',y''}$ where

$$z' = \sum_{\substack{0\le h\le p\\ 2|h}} \binom{p}{h} z^{p-h}y^h\epsilon^{\frac{h}{2}}$$

and

$$y'' = \sum_{\substack{0\le h\le p\\ 2|h}} \binom{p}{h} z^{p-h}y^h\epsilon^{\frac{h-1}{2}}$$

So $\psi_n((t^0_{w,y})^p)$ and $\psi_n((k^0_{z,y})^p)$ are equal to $\varphi(\psi_n(t^0_{w,y}))$ and $\varphi(\psi_n(k^0_{z,y}))$ respectively (this will be useful when calculating $(f\circ\psi_n)(t^0_{w,y})$ and $(f\circ\psi_n)(k^0_{z,y})$ respectively).

$$\begin{aligned}
(rci^{j,i}_{x,\alpha})^p &= \begin{pmatrix} x & p^i\alpha \\ p^j\alpha & x\end{pmatrix}^p = \left(\begin{pmatrix} x & 0 \\ 0 & x\end{pmatrix} + \begin{pmatrix} 0 & p^i\alpha \\ p^j\alpha & 0\end{pmatrix}\right)^p \\
&= \sum_{h=0}^{p}\binom{p}{h}\begin{pmatrix} x & 0 \\ 0 & x\end{pmatrix}^{p-h}\begin{pmatrix} 0 & p^i\alpha \\ p^j\alpha & 0\end{pmatrix}^h \\
&= \sum_{\substack{0\le h\le p\\ 2|h}}\binom{p}{h}\begin{pmatrix} x^{p-h}(p^{i+j}\alpha^2)^{\frac{h}{2}} & 0 \\ 0 & x^{p-h}(p^{i+j}\alpha^2)^{\frac{h}{2}}\end{pmatrix} \\
&\quad + \sum_{\substack{0\le h\le p\\ 2|h}}\binom{p}{h}\begin{pmatrix} 0 & x^{p-h}(p^{i+j}\alpha^2)^{\frac{h-1}{2}}p^i\alpha \\ x^{p-h}(p^{i+j}\alpha^2)^{\frac{h-1}{2}}p^j\alpha & 0\end{pmatrix} \\
&= \begin{pmatrix} x^p+O(p) & x^{p-1}p^{i+1}\alpha+O(p^{i+2}) \\ x^{p-1}p^{j+1}\alpha+O(p^{j+2}) & x^p+O(p)\end{pmatrix}
\end{aligned}$$

Where $O(q)$ stands for an element divisible by $q$. Since $p$ does not divide $x$ or $\alpha$, we can conclude that, for $i = n-1$, $(rci^{j,i}_{x,\alpha})^p = rc^{j+1}_{x^p,\alpha x^{p-1}}$, and for $i < n-1$, $(rci^{j,i}_{x,\alpha})^p = rci^{j+1,i+1}_{x',\alpha'}$, for some $x' \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $\alpha' \in (\mathbb{Z}/p^{n-i}\mathbb{Z})^\times$. So $\psi_n((rci^{j,i}_{x,\alpha})^p)$ is equal to $p^2\varphi(\psi_n(rci^{j,i}_{x,\alpha}))$ for $i < n-1$. This is similar[3]for $rcj^{j,i}_{x,\alpha}$, $rt^i_{x,\alpha}$, $rk^i_{x,\alpha}$, $ri^j_{x,\beta}$ and $rj^j_{x,\beta}$.

[3]If $i,j < n-1$ we have $(rcj^{j,i}_{x,\alpha})^p = rcj^{j+1,i+1}_{x',\alpha'}$, $(rt^i_{x,\alpha})^p = rci^{1,i+1}_{x',\alpha'}$, $(rk^i_{x,\alpha})^p = rcj^{1,i+1}_{x',\alpha'}$, $(ri^j_{x,\beta})^p = ri^{j+1}_{x',\beta'}$ and $(rj^j_{x,\beta})^p = rj^{j+1}_{x',\beta'}$.

Otherwise we have $(rcj^{j,n-1}_{x,\alpha})^p = rc^{j+1}_{x^p,\alpha x^{p-1}}$, $(rt^{n-1}_{x,\alpha})^p = rc^1_{x^p,\alpha x^{p-1}}$, $(rk^{n-1}_{x,\alpha})^p = rc^1_{x^p,\alpha x^{p-1}}$, $(ri^{n-1}_{x,\beta})^p = i_{x^p}$ and $(rj^{n-1}_{x,\beta})^p = i_{x^p}$.

| $A$ | $\psi_n(A)$ |
|---|---|
| $i_x$ | $([G_n : U]i_x)_{\mathcal{F}_n}$ |
| $c^0_{x,1}$ | $\left(\sum_{y\in(\mathbb{Z}/p^n\mathbb{Z})^\times} c^0_{x,y}\right)_{C_n}$ |
| $t^0_{w,y}$ | $\left(t^0_{w,y} + t^0_{w,-y}\right)_{T_n}$ |
| $k^0_{z,y}$ | $\left(k^0_{z,y} + k^0_{z,-y}\right)_{K_n}$ |
| $rt^i_{x,\alpha}$ | $\left(rt^i_{x,\alpha} + rt^i_{x,-\alpha}\right)_{N_{t^i}}$ |
| $rk^i_{x,\alpha}$ | $\left(rk^i_{x,\alpha} + rk^i_{x,-\alpha}\right)_{N_{k^i}}$ |
| $rc^j_{x,1}$ | $\left(p^{2j}\sum_{\beta\in(\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} rc^j_{x,\beta}\right)_{C_n\times\prod_{i=n-j}^{n-1}(N_{t^i}\times N_{k^i})}$ |
| $rci^{j,i}_{x,\alpha}$ | $\left(p^{2j}(rci^{j,i}_{x,\alpha} + rci^{j,i}_{x,-\alpha})\right)_{N_{t^{i-j}}}$ |
| $rcj^{j,i}_{x,\alpha}$ | $\left(p^{2j}(rcj^{j,i}_{x,\alpha} + rcj^{j,i}_{x,-\alpha})\right)_{N_{k^{i-j}}}$ |
| $ri^j_{x,\beta}$ | $\left(p^{2j}(ri^j_{x,\beta} + ri^j_{x,-\beta})\right)_{T_n}$ |
| $rj^j_{x,\beta}$ | $\left(p^{2j}(rj^j_{x,\beta} + rj^j_{x,-\beta})\right)_{K_n}$ |

In most cases it is straight forward to calculate $(f\circ\psi_n)(A)$ since $\psi_U(A)$ is non-zero for only one subgroup $U\in\mathcal{F}_n$. The greatest exception is $A = i_x$, so we will explicitly do this case:
Set $\psi(A) = (a_U)_{U\in\mathcal{F}_n}$ then we have $a_U = [G_n : U][i_x]$ thus we have $Tr_{U/Z_n}(a_U) = [U : Z_n][G_n : U][i_x]$ therefore we have $T_U(a_U) = [G_n : U][i_x] = a_U$. Therefore $\lambda_f((a_V)) = 0$ and, for a similar reason we get $\mu_{f,N}(a_N) = 0 = \nu_{f,N}(a_{C_n})$ for all $N\in\{N_{t^i}, N_{k^i} | i = 1, 2, ..., n-1\}$. So we clearly get $(f_U\circ\psi_n)(A) = [G_n : U](i_x - i_{x^p}/p)$ for the cases $U = Z_n, T_n, K_n$. In the case $U = N_{t^i}, N_{k^i}$ we have:

$$(f_U\circ\psi_n)(A) = a_U - p\varphi(a_U) - \frac{1}{p}\varphi\left(T_U(a_U)\right) + p\varphi\left(T_U(a_U)\right)$$

which also simplifies to $[G_n : U](i_x - i_{x^p}/p)$. Finally, in the case $U = C_n$ we have:

$$(f_{C_n}\circ\psi_n)(A) = a_{C_n} - \varphi(a_{C_n}) - \frac{1}{p}\varphi\left(T_{C_n}(a_{C_n})\right) + T_{C_n}(\varphi(a_{C_n}))$$

which also simplifies to $[G_n : U](i_x - i_{x^p}/p)$, therefore $(f\circ\psi_n)(A) = ([G_n : U](i_x - i_{x^p}/p))_{\mathcal{F}_n}$

The rest of the cases are in this table:

| $A$ | $(f\circ\psi_n)(A)$ |
|---|---|
| $i_x$ | $([G_n : U](i_x - i_{x^p}/p))_{\mathcal{F}_n}$ |
| $c^0_{x,1}$ | $\left(\sum_{y\in(\mathbb{Z}/p^n\mathbb{Z})^\times} c^0_{x,y} - p\sum_{\beta\in(\mathbb{Z}/p^{n-1}\mathbb{Z})^\times} rc^1_{x^p,\beta}\right)_{C_n}$ |
| $t^0_{w,y}$ | $\left(t^0_{w,y} + t^0_{w,-y} - \frac{\psi_n((t^0_{w,y})^p)}{p}\right)_{T_n}$ |
| $k^0_{z,y}$ | $\left(k^0_{z,y} + k^0_{z,-y} - \frac{\psi_n((k^0_{z,y})^p)}{p}\right)_{K_n}$ |
| $rt^i_{x,\alpha}$ for $i < n-1$ | $\left(rt^i_{x,\alpha} + rt^i_{x,-\alpha} - \frac{\psi_n((rt^i_{x,\alpha})^p)}{p}\right)_{N_{t^i}}$ |
| $rt^{n-1}_{x,\alpha}$ | $\left(rt^{n-1}_{x,\alpha} + rt^{n-1}_{x,-\alpha} - p\sum_{\beta\in(\mathbb{Z}/p^{n-1}\mathbb{Z})^\times} rc^1_{x^p,\beta},\ -p\sum_{\beta\in(\mathbb{Z}/p^{n-1}\mathbb{Z})^\times} rc^1_{x^p,\beta}\right)_{N_{t^{n-1}},C_n\times N_{k^{n-1}}}$ |

| | |
|---|---|
| $rk^i_{x,\alpha}$ for $i < n-1$ | $\left(rk^i_{x,\alpha} + rk^i_{x,-\alpha} - \frac{\psi_n((rk^i_{x,\alpha})^p)}{p}\right)_{N_{k^i}}$ |
| $rk^{n-1}_{x,\alpha}$ | $\Big(rk^{n-1}_{x,\alpha} + rk^{n-1}_{x,-\alpha} - p \sum_{\beta\in(\mathbb{Z}/p^{n-1}\mathbb{Z})^\times} rc^1_{x^p,\beta}, -p \sum_{\beta\in(\mathbb{Z}/p^{n-1}\mathbb{Z})^\times} rc^1_{x^p,\beta}\Big)_{N_{k^{n-1}}, C_n\times N_{t^{n-1}}}$ |
| $rc^j_{x,1}$ for $j < n-1$ | $\Big(p^{2j} \sum_{\beta\in(\mathbb{Z}/p^{n-j}\mathbb{Z})^\times} rc^j_{x,\beta} - p^{2j+1} \sum_{\beta\in(\mathbb{Z}/p^{n-j-1}\mathbb{Z})^\times} rc^{j+1}_{x^p,\beta}, -p^{2j+1} \sum_{\beta\in(\mathbb{Z}/p^{n-j-1}\mathbb{Z})^\times} rc^{j+1}_{x^p,\beta}\Big)_{C_n\times \prod_{i=n-j}^{n-1}(N_{t^i}\times N_{k^i}), N_{t^{n-j-1}}\times N_{k^{n-j-1}}}$ |
| $rc^{n-1}_{x,1}$ | $\Big(p^{2n-2} \sum_{\beta\in(\mathbb{Z}/p\mathbb{Z})^\times} rc^{n-1}_{x,\beta} - \frac{[G_n:C_n]}{p} i_{x^p}, -\frac{[G_n:U]}{p} i_{x^p}\Big)_{C_n\times \prod_{i=1}^{n-1}(N_{t^i}\times N_{k^i}), \mathcal{F}_n\setminus(C_n\times \prod_{i=1}^{n-1}(N_{t^i}\times N_{k^i}))}$ |
| $rci^{j,i}_{x,\alpha}$ for $i < n-1$ | $\left(p^{2j}(rci^{j,i}_{x,\alpha} + rci^{j,i}_{x,-\alpha}) - \frac{\psi_n((rci^{j,i}_{x,\alpha})^p)}{p}\right)_{N_{t^{i-j}}}$ |
| $rci^{j,n-1}_{x,\alpha}$ | $\Big(p^{2j}(rci^{j,n-1}_{x,\alpha} + rci^{j,n-1}_{x,-\alpha}) - p^{2j+1} \sum_{\beta\in(\mathbb{Z}/p^{n-j-1}\mathbb{Z})^\times} rc^{j+1}_{x^p,\beta}, -p^{2j+1} \sum_{\beta\in(\mathbb{Z}/p^{n-j-1}\mathbb{Z})^\times} rc^{j+1}_{x^p,\beta}\Big)_{N_{t^{n-1-j}}, C_n\times N_{k^{n-1-j}}\times \prod_{i=n-j}^{n-1}(N_{t^i}\times N_{k^i})}$ |
| $rcj^{j,i}_{x,\alpha}$ for $i < n-1$ | $\left(p^{2j}(rcj^{j,i}_{x,\alpha} + rcj^{j,i}_{x,-\alpha}) - \frac{\psi_n((rcj^{j,i}_{x,\alpha})^p)}{p}\right)_{N_{k^{i-j}}}$ |
| $rcj^{j,n-1}_{x,\alpha}$ | $\Big(p^{2j}(rcj^{j,i}_{x,\alpha} + rcj^{j,i}_{x,-\alpha})) - p^{2j+1} \sum_{\beta\in(\mathbb{Z}/p^{n-j-1}\mathbb{Z})^\times} rc^{j+1}_{x^p,\beta}, -p^{2j+1} \sum_{\beta\in(\mathbb{Z}/p^{n-j-1}\mathbb{Z})^\times} rc^{j+1}_{x^p,\beta}\Big)_{N_{k^{n-1-j}}, C_n\times N_{t^{n-1-j}}\times \prod_{i=n-j}^{n-1}(N_{t^i}\times N_{k^i})}$ |
| $ri^j_{x,\beta}$ for $j < n-1$ | $\left(p^{2j}(ri^j_{x,\beta} + ri^j_{x,-\beta}) - \frac{\psi_n((ri^j_{x,\beta})^p)}{p}\right)_{T_n}$ |
| $ri^{n-1}_{x,\beta}$ | $\left(p^{2n-2}(ri^{n-1}_{x,\beta} + ri^{n-1}_{x,-\beta}) - \frac{[G_n:T_n]}{p} i_{x^p}, -\frac{[G_n:U]}{p} i_{x^p}\right)_{T_n, \mathcal{F}_n\setminus T_n}$ |
| $rj^j_{x,\beta}$ for $j < n-1$ | $\left(p^{2j}(rj^j_{x,\beta} + rj^j_{x,-\beta}) - \frac{\psi_n((rj^j_{x,\beta})^p)}{p}\right)_{K_n}$ |
| $rj^{n-1}_{x,\beta}$ | $\left(p^{2n-2}(rj^{n-1}_{x,\beta} + rj^{n-1}_{x,-\beta}) - \frac{[G_n:K_n]}{p} i_{x^p}, -\frac{[G_n:U]}{p} i_{x^p}\right)_{K_n, \mathcal{F}_n\setminus K_n}$ |

$$i, j = 1, 2, ..., n-1 \text{ s.t } j < i,\ x, y \in (\mathbb{Z}/p^n\mathbb{Z})^\times \text{ and } w, z \in \mathbb{Z}/p^n\mathbb{Z} \text{ s.t } y \not\equiv \pm w\ (mod\ p)$$

$$k, l \in \mathbb{Z}/p^j\mathbb{Z}, \alpha \in (\mathbb{Z}/p^{n-i}\mathbb{Z})^\times \text{ and } \beta \in (\mathbb{Z}/p^{n-j}\mathbb{Z})^\times$$

This table and the table for $\psi_n \circ (1 - \frac{\varphi}{p})$ show that the above diagram is commutative for our choice of $f$, and as a result diagram (1), from chapter 2.6.2, is also commutative for $\mathcal{L} = f \circ log$.

□

## 5.2 Obtaining an explicit description of $\mathcal{L}$

We set $\mathcal{L} = f \circ log$ so, to find an explicit description for $\mathcal{L}$, we just write $\mathcal{L} = \prod_{U\in\mathcal{F}} \mathcal{L}_U$ such that $\mathcal{L}_U = f_U \circ log$ i.e. we just replace $a_U$ with $log(x_U)$ in the definition of $f_U$:

### Case $U = N_{t^i}$ or $N_{k^i}$

In the case that $U = N_{t^i}$ or $N_{k^i}$ we have

$$\begin{aligned} f_U &= a_U - p\varphi(a_U) - \tfrac{1}{p}\varphi\left(T_U(a_U)\right) + p\varphi\left(T_U(a_U)\right) - [G_n : U]\lambda_f((a_V)) \\ &\quad - \sum_{\substack{N=N_{t^l},N_{k^l} \\ l\leq i}} \mu_{f,N}(a_N)\sum_\beta rc_{1,\beta}^{n-l} + \mu_{f,U}(a_U)\sum_\beta rc_{1,\beta}^{n-i} + \nu_{f,U}(a_{C_n}) \end{aligned}$$

where $T_U(a_U) = \frac{Tr_{U/Z_n}(a_U)}{[W:Z_n]}$ and:

$$\lambda_f((a_V)) = \frac{1}{p}\sum_{W=C_n,T_n,K_n} \frac{Tr_{W/Z_n}\left(\varphi\left(a_W - T_W(a_W)\right)\right)}{[W:Z_n]}$$

$$\mu_{f,N}(a_N) = \frac{p}{2}\varphi\left(\frac{Tr_{N/(Z_{n-i-1}\cap N)}(a_N)}{[N:Z_{n-i-1}\cap N]} - \frac{Tr_{N/(Z_{n-i}\cap N)}(a_N)}{[N:Z_{n-i}\cap N]}\right)$$

$$\nu_{f,N}(a_{C_n}) = Tr_{C_n/(Z_{n-i}\cap C_n)}\Big(a_{C_n} - \varphi(a_{C_n}) - T_{C_n}(a_{C_n}) + T_{C_n}(\varphi(a_{C_n}))\Big)$$

So $\mathcal{L}_U$ would be defined as:

$$\begin{aligned} &log(x_U) - p\varphi(log(x_U)) - \tfrac{1}{p}\varphi\left(T_U(log(x_U))\right) + p\varphi\left(T_U(log(x_U))\right) - [G_n : U]\lambda_f(log((x_V))) \\ &- \sum_{\substack{N=N_{t^l},N_{k^l} \\ l\leq i}} \mu_{f,N}(log(x_N))\sum_\beta rc_{1,\beta}^{n-l} + \mu_{f,U}(log(x_U))\sum_\beta rc_{1,\beta}^{n-i} + \nu_{f,U}(log(x_{C_n})) \end{aligned}$$

We can simplify $T_U(log(x_U))$ to $log(N_U(x_U))$ where $N_U(x_U) = Nm_{U/Z_n}(x_U)^{\frac{1}{[U:Z_n]}}$.
We can also simplify $\lambda_f(log((x_V)))$, $\mu_{f,N}(log(x_N))$ and $\nu_{f,N}(log(x_{C_n}))$ but we will start with $\lambda_f(log((x_V)))$:

$$\begin{aligned} &\tfrac{1}{p}\textstyle\sum_{W=C_n,T_n,K_n} \frac{Tr_{W/Z_n}\left(\varphi\left(log(x_W) - \frac{Tr_{W/Z_n}(log(x_W))}{[W:Z_n]}\right)\right)}{[W:Z_n]} \\ = \;& \tfrac{1}{p}\textstyle\sum_{W=C_n,T_n,K_n} \frac{Tr_{W/Z_n}\left(\frac{1}{[W:Z_n]}\left([W:Z_n]\varphi(log(x_W)) - \varphi(log(Nm_{W/Z_n}(x_W)))\right)\right)}{[W:Z_n]} \\ = \;& -\tfrac{1}{p}\textstyle\sum_{W=C_n,T_n,K_n} \frac{1}{[W:Z_n]^2} Tr_{W/Z_n}\left(log\left(\frac{\varphi(Nm_{W/Z_n}(x_W))}{\varphi(x_W)^{[W:Z_n]}}\right)\right) \\ = \;& -\tfrac{1}{p}\textstyle\sum_{W=C_n,T_n,K_n} \frac{1}{[W:Z_n]^2} log\left(Nm_{W/Z_n}\left(\frac{\varphi(Nm_{W/Z_n}(x_W))}{\varphi(x_W)^{[W:Z_n]}}\right)\right) \\ = \;& -\tfrac{1}{[G_n:U]p} log\left(\lambda_{\mathcal{L},U}((x_V))\right) \end{aligned}$$

where $\lambda_{\mathcal{L},U}((x_V)) = \prod_{W=C_n,T_n,K_n} Nm_{W/Z_n}\left(\frac{\varphi(Nm_{W/Z_n}(x_W))}{\varphi(x_W)^{[W:Z_n]}}\right)^{\frac{[G_n:U]}{[W:Z_n]^2}}$.
Now we will simplify our expression for $\mu_{f,N}(log(x_N))$:

$$\begin{aligned} &\tfrac{p}{2}\varphi\left(\frac{Tr_{N/(Z_{n-i-1}\cap N)}(log(x_N))}{[N:Z_{n-i-1}\cap N]} - \frac{Tr_{N/(Z_{n-i}\cap N)}(log(x_N))}{[N:Z_{n-i}\cap N]}\right) \\ = \;& \tfrac{p}{2}\varphi\left(\tfrac{1}{[N:Z_{n-i}\cap N]}\left(plog(Nm_{N/(Z_{n-i-1}\cap N)}(x_N)) - log(Nm_{N/(Z_{n-i}\cap N)}(x_N))\right)\right) \\ = \;& \tfrac{p}{2[N:Z_{n-i}\cap N]} log\left(\varphi\left(\frac{Nm_{N/(Z_{n-i-1}\cap N)}(x_N)^p}{Nm_{N/(Z_{n-i}\cap N)}(x_N)}\right)\right) \\ = \;& \mu_{\mathcal{L},N}(x_N) \end{aligned}$$

where $\mu_{\mathcal{L},N}(x_N) = log\left(\varphi\left(\frac{Nm_{N/(Z_{n-i-1}\cap N)}(x_N)^p}{Nm_{N/(Z_{n-i}\cap N)}(x_N)}\right)^{\frac{p}{2[N:Z_{n-i}\cap N]}}\right)$.
Finally we will simplify our expression for $\nu_{f,N}(log(x_{C_n}))$:

$$\begin{aligned}
& Tr_{C_n/(Z_{n-i}\cap C_n)}\Big(log(x_{C_n}) - \varphi(log(x_{C_n})) - T_{C_n}(log(x_{C_n})) + T_{C_n}(\varphi(log(x_{C_n})))\Big) \\
= \; & -Tr_{C_n/(Z_{n-i}\cap C_n)}\Big(-log(x_{C_n}) + log(\varphi(x_{C_n})) + log(N_{C_n}(x_{C_n})) - log(N_{C_n}(\varphi(x_{C_n})))\Big) \\
= \; & -Tr_{C_n/(Z_{n-i}\cap C_n)}\left(log\left(\tfrac{N_{C_n}(x_{C_n})\varphi(x_{C_n})}{x_{C_n}N_{C_n}(\varphi(x_{C_n}))}\right)\right) \\
= \; & -\tfrac{1}{p}log(\nu_{\mathcal{L},N}(x_{C_n}))
\end{aligned}$$

where $\nu_{\mathcal{L},N}(x_{C_n}) = Nm_{C_n/(Z_{n-i}\cap C_n)}\left(\frac{N_{C_n}(x_{C_n})\varphi(x_{C_n})}{x_{C_n}N_{C_n}(\varphi(x_{C_n}))}\right)^p$.
Now we can simplify our expression for $\mathcal{L}_U$ in the case that $U = N_{t^i}$ or $N_{k^i}$:

$$\begin{aligned}
& log(x_U) - p\varphi(log(x_U)) - \tfrac{1}{p}\varphi\left(T_U(log(x_U))\right) + p\varphi\left(T_U(log(x_U))\right) - [G_n : U]\lambda_f(log((x_V))) \\
& - \sum_{\substack{N=N_{t^l},N_{k^l} \\ l\le i}} \mu_{f,N}(log(x_N))\sum_\beta rc_{1,\beta}^{n-l} + \mu_{f,U}(log(x_U))\sum_\beta rc_{1,\beta}^{n-i} + \nu_{f,U}(log(x_{C_n})) \\
= \; & log(x_U) - log((\varphi(x_U))^p) - \tfrac{1}{p}log(\varphi(N_U(x_U))) + log(\varphi(N_U(x_U))^p) + log(\lambda_{\mathcal{L},U}((x_V))) \\
& - \sum_{\substack{N=N_{t^l},N_{k^l} \\ l\le i}} \mu_{\mathcal{L},N}(x_N)\sum_\beta rc_{1,\beta}^{n-l} + \mu_{\mathcal{L},U}(x_U)\sum_\beta rc_{1,\beta}^{n-i} - \tfrac{1}{p}log(\nu_{\mathcal{L},U}(x_{C_n})) \\
= \; & \tfrac{1}{p}log\left(\frac{x_U^p\varphi(N_U(x_U))^{p^2}\lambda_{\mathcal{L},U}((x_V))}{\varphi(x_U)^{p^2}\varphi(N_U(x_U))\nu_{\mathcal{L},U}(x_{C_n})}\right) - \sum_{\substack{N=N_{t^l},N_{k^l} \\ l\le i}} \mu_{\mathcal{L},N}(x_N)\sum_\beta rc_{1,\beta}^{n-l} + \mu_{\mathcal{L},U}(x_U)\sum_\beta rc_{1,\beta}^{n-i}
\end{aligned}$$

## Case $U = C_n$

For the $U = C_n$ case, we have

$$\begin{aligned}
f_{C_n} \; = \; & a_{C_n} - \varphi(a_{C_n}) - \tfrac{1}{p}\varphi\left(T_{C_n}(a_{C_n})\right) + T_{C_n}(\varphi(a_{C_n})) \\
& -[G_n : C_n]\lambda_f((a_V)) - \sum_{N=N_{t^i},N_{k^i}} \mu_{f,N}(a_N)\sum_\beta rc_{1,\beta}^{n-i}
\end{aligned}$$

So $\mathcal{L}_{C_n}$ is defined as:

$$\begin{aligned}
& log(x_{C_n}) - \varphi(log(x_{C_n})) - \tfrac{1}{p}\varphi\left(T_{C_n}(log(x_{C_n}))\right) + T_{C_n}(\varphi(log(x_{C_n})) \\
& -[G_n : C_n]\lambda_f((log(x_V))) - \sum_{N=N_{t^i},N_{k^i}} \mu_{f,N}(log(x_N))\sum_\beta rc_{1,\beta}^{n-i} \\
= \; & log(x_{C_n}) - log(\varphi(x_{C_n})) - \tfrac{1}{p}log\left(\varphi\left(N_{C_n}(x_{C_n})\right)\right) + log(N_{C_n}(\varphi(x_{C_n}))) \\
& + \tfrac{1}{p}log(\lambda_{\mathcal{L},C_n}((x_V))) - \sum_{N=N_{t^i},N_{k^i}} \mu_{\mathcal{L},N}(x_N)\sum_\beta rc_{1,\beta}^{n-i} \\
= \; & \tfrac{1}{p}log\left(\frac{x_{C_n}^p N_{C_n}(\varphi(x_{C_n}))^p\lambda_{\mathcal{L},C_n}((x_V))}{\varphi(x_{C_n})^p\varphi\left(N_{C_n}(x_{C_n})\right)}\right) - \sum_{N=N_{t^i},N_{k^i}} \mu_{\mathcal{L},N}(x_N)\sum_\beta rc_{1,\beta}^{n-i}
\end{aligned}$$

where $\sum_\beta$ is a sum of all $\beta \in (\mathbb{Z}/p^i\mathbb{Z})^\times$.

### Case $U = Z_n, T_n$ or $K_n$

In the case $U = Z_n$, $f_{Z_n} = a_{Z_n} - \frac{\varphi(a_{Z_n})}{p} - [G_n : Z_n]\lambda_f((a_V))$, so $\mathcal{L}_{Z_n}$ is defined as:

$$\begin{aligned} & log(x_{Z_n}) - \tfrac{\varphi(log(x_{Z_n}))}{p} - [G_n : Z_n]\lambda_f(log((x_V))) \\ = \quad & log(x_{Z_n}) - \tfrac{1}{p}log(\varphi(x_{Z_n})) + \tfrac{1}{p}log(\lambda_{\mathcal{L},Z_n}((x_V))) \\ = \quad & \tfrac{1}{p}log\left(\tfrac{x_{Z_n}^p \lambda_{\mathcal{L},Z_n}((x_V))}{\varphi(x_{Z_n})}\right) \end{aligned}$$

Finally, in the case $U = T_n$ or $K_n$, $f_U = a_U - \frac{\varphi(a_U)}{p} + \frac{1}{p}\Big(T_U(\varphi(a_U)) - \varphi(T_U(a_U))\Big) - [G_n : U]\lambda_f((a_V))$, so $\mathcal{L}_U$ is defined as:

$$\begin{aligned} & log(x_U) - \tfrac{\varphi(log(x_U))}{p} + \tfrac{1}{p}\Big(T_U(\varphi(log(x_U))) - \varphi(T_U(log(x_U)))\Big) - [G_n : U]\lambda_f(log((x_V))) \\ = \quad & log(x_U) - \tfrac{1}{p}log(\varphi(x_U)) + \tfrac{1}{p}log(N_U(\varphi(x_U))) - \tfrac{1}{p}log(\varphi(N_U(x_U))) + \tfrac{1}{p}log(\lambda_{\mathcal{L},U}((x_V))) \\ = \quad & \tfrac{1}{p}log\left(\tfrac{x_U^p N_U(\varphi(x_U))\lambda_{\mathcal{L},U}((x_V))}{\varphi(x_U)\varphi(N_U(x_U))}\right) \end{aligned}$$

Now it is very easy to state $\mathcal{L}$:
$\mathcal{L} = \prod_{U\in\mathcal{F}} \mathcal{L}_U$ such that

$$\mathcal{L}_U((x_V)) := \begin{cases} \tfrac{1}{p}log\left(\tfrac{x_U^p \varphi(N_U(x_U))^{p^2}\lambda_{\mathcal{L},U}((x_V))}{\varphi(x_U)^{p^2}\varphi(N_U(x_U))\nu_{\mathcal{L},U}(x_{C_n})}\right) & \\ -\sum\limits_{\substack{N=N_{tl},N_{kl} \\ l\le i}} \mu_{\mathcal{L},N}(x_N) \sum\limits_{\beta\in(\mathbb{Z}/p^l\mathbb{Z})^\times} rc_{1,\beta}^{n-l} & \\ +\mu_{\mathcal{L},U}(x_U) \sum\limits_{\beta\in(\mathbb{Z}/p^i\mathbb{Z})^\times} rc_{1,\beta}^{n-i} & \text{if } U = N_{t^i} \text{ or } N_{k^i} \\ \tfrac{1}{p}log\left(\tfrac{x_{C_n}^p N_{C_n}(\varphi(x_{C_n}))^p \lambda_{\mathcal{L},C_n}((x_V))}{\varphi(x_{C_n})^p \varphi\big(N_{C_n}(x_{C_n})\big)}\right) & \\ -\sum\limits_{N=N_{t^i},N_{k^i}} \mu_{\mathcal{L},N}(x_N) \sum\limits_{\beta\in(\mathbb{Z}/p^i\mathbb{Z})^\times} rc_{1,\beta}^{n-i} & \text{if } U = C_n \\ \tfrac{1}{p}log\left(\tfrac{x_{Z_n}^p \lambda_{\mathcal{L},Z_n}((x_V))}{\varphi(x_{Z_n})}\right) & \text{if } U = Z_n \\ \tfrac{1}{p}log\left(\tfrac{x_U^p N_U(\varphi(x_U))\lambda_{\mathcal{L},U}((x_V))}{\varphi(x_U)\varphi(N_U(x_U))}\right) & \text{if } U = T_n \text{ or } K_n \end{cases}$$

Where $N_U(x_U) = Nm_{U/Z_n}(x_U)^{\frac{1}{[U:Z_n]}}$, $\lambda_{\mathcal{L},U}$ is a map from $\prod_{U\in\mathcal{F}_n} \mathbb{Z}_p[U]^\times$ to $\mathbb{Q}_p^\times \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[Z_n]^\times$, $\mu_{\mathcal{L},N}$ is a map from $\mathbb{Z}_p[N]^\times$ to $\mathbb{Q}_p^\times \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[Z_{n-i} \cap C_n]^\times$ and $\nu_{\mathcal{L},N}$ is a map from $\mathbb{Z}_p[C_n]^\times$ to $\mathbb{Q}_p^\times \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[N]^\times$ for $N \in \{N_{t^i}, N_{k^i} | i = 1, 2, ..., n-1\}$. These maps are defined in the following way:

$$\lambda_{\mathcal{L},U}((x_V)) = \prod_{W=C_n,T_n,K_n} Nm_{W/Z_n}\left(\frac{\varphi(Nm_{W/Z_n}(x_W))}{\varphi(x_W)^{[W:Z_n]}}\right)^{\frac{[G_n:U]}{[W:Z_n]^2}}$$

$$\mu_{\mathcal{L},N}(x_N) = log\left(\varphi\left(\frac{Nm_{N/(Z_{n-i-1}\cap N)}(x_N)^p}{Nm_{N/(Z_{n-i}\cap N)}(x_N)}\right)^{\frac{p}{2[N:Z_{n-i}\cap N]}}\right)$$

$$\nu_{\mathcal{L},N}(x_{C_n}) = Nm_{C_n/(Z_{n-i}\cap C_n)}\left(\frac{N_{C_n}(x_{C_n})\varphi(x_{C_n})}{x_{C_n}N_{C_n}(\varphi(x_{C_n}))}\right)^p$$

Note that $Z_n$ is a subgroup of any $U \in \mathcal{F}_n$, so any element $x_{Z_n} \in \mathbb{Z}_p[Z_n]^\times$ can also be thought as an element of $\mathbb{Z}_p[U]^\times$. In particular, for any $U \in \mathcal{F}_n$, we have $\lambda_{\mathcal{L},U}((x_V)) \in \mathbb{Q}_p^\times \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[U]^\times$. Also note that $Z_{n-i} \cap C_n = Z_{n-i} \cap N$ for $N \in \{N_{t^i}, N_{k^i} | i = 1, 2, ..., n-1\}$ so we have both $\mu_{\mathcal{L},N} \in \mathbb{Q}_p^\times \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[Z_{n-i} \cap C_n]^\times$ and $\mu_{\mathcal{L},N} \in \mathbb{Q}_p^\times \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[Z_{n-i} \cap N]^\times$.

## 5.3 Finding the group $\Theta_{n,\mathbb{Z}_p}$

Now we can easily find conditions for a group $\Theta_{n,\mathbb{Z}_p} \subset \prod_{U \in \mathcal{F}_n} \Lambda(U^{ab})^\times$ such that $\Psi_{n,\mathbb{Z}_p} \subset \mathcal{L}(\Theta_{n,\mathbb{Z}_p})$ Recall that $N_V(U)$ denotes the normalizer of $U$ as a subgroup of $V$. Now recall the definition of $\Psi_{n,R}$:
Let $R$ be a $\mathbb{Z}_p$-algebra of characteristic 0. $\Psi_{n,R}$ is defined using the following conditions:

1. $\Psi_{n,R} \subset p^{3n-2}R[Z_n] \times R[C_n] \times R[T_n] \times R[K_n] \times \prod_{i=1}^{n-1} (R[N_{t^i}] \times R[N_{k^i}])$
2. For any $(a_V)_{V \in \mathcal{F}_n} \in \Psi_{n,R}$, each $a_V$ is fixed by conjugation action of $N_{G_n}(V)$
3. For any $(a_V)_{V \in \mathcal{F}_n} \in \Psi_{n,R}$, we have:
   - $Tr_{V/Z_n}(a_V) = a_{Z_n}$ for all $V \in \mathcal{F}_n$
   - $Tr_{N_{t^i}/Z_m \cap N_{t^i}}(a_{N_{t^i}}) = Tr_{C_n/Z_m \cap C_n}(a_{C_n})$ for $m \geq n - i$
   - $Tr_{N_{k^i}/Z_m \cap N_{k^i}}(a_{N_{k^i}}) = Tr_{C_n/Z_m \cap C_n}(a_{C_n})$ for $m \geq n - i$
4. For any $(a_V)_{V \in \mathcal{F}_n} \in \Psi_{n,R}$, we have:
   - $Tr_{C_n/Z_m \cap C_n}(a_{C_n}) \in p^{3m}R[C_n]$
   - $Tr_{T_n/Z_m \cap T_n}(a_{T_n}) \in p^{3m-1}R[T_n]$
   - $Tr_{K_n/Z_m \cap K_n}(a_{K_n}) \in p^{3m-1}R[K_n]$
   - $Tr_{N_{t^i}/Z_m \cap N_{t^i}}(a_{N_{t^i}}) \in p^{3m}R[N_{t^i}]$
   - $Tr_{N_{k^i}/Z_m \cap N_{k^i}}(a_{N_{k^i}}) \in p^{3m}R[N_{k^i}]$

Now we define $\Theta_{n,R}$:

**Definition 5.1** *First recall the maps:*

$$\lambda_{\mathcal{L},U}((x_V)) = \prod_{W=C_n,T_n,K_n} Nm_{W/Z_n}\left(\frac{\varphi(Nm_{W/Z_n}(x_W))}{\varphi(x_W)^{[W:Z_n]}}\right)^{\frac{[G_n:U]}{[W:Z_n]^2}}$$

$$\mu_{\mathcal{L},N}(x_N) = log\left(\varphi\left(\frac{Nm_{N/(Z_{n-i-1}\cap N)}(x_N)^p}{Nm_{N/(Z_{n-i}\cap N)}(x_N)}\right)^{\frac{p}{2[N:Z_{n-i}\cap N]}}\right)$$

$$\nu_{\mathcal{L},N}(x_{C_n}) = Nm_{C_n/(Z_{n-i}\cap C_n)}\left(\frac{N_{C_n}(x_{C_n})\varphi(x_{C_n})}{x_{C_n}N_{C_n}(\varphi(x_{C_n}))}\right)^p$$

*Let $R$ be a $\mathbb{Z}_p$-algebra of characteristic 0. We define $\Theta_{n,R}$ using the following conditions:*

1. *$\Theta_{n,R} \subset \prod_{U \in \mathcal{F}_n} R[U]^\times$ such that $x_{Z_n}^p\left(\lambda_{\mathcal{L},Z_n}((x_V)_{V \in \mathcal{F}_n})\right) \equiv \varphi(x_{Z_n})\ (mod\ p^{3n-1})$*
2. *For any $(x_V)_{V \in \mathcal{F}_n} \in \Theta_{n,R}$, each $x_V$ is fixed by conjugation action of $N_{G_n}(V)$*
3. *For any $(x_V)_{V \in \mathcal{F}_n} \in \Theta_{n,R}$, we have:*
   - *$Nm_{V/Z_n}(x_V) = x_{Z_n}$ for all $V \in \mathcal{F}_n$*

- $\frac{1}{p}log\left(Nm_{U/Z_m\cap U}\left(\frac{x_U^p\varphi(N_U(x_U))^{p^2}\lambda_{\mathcal{L},U}((x_V))}{\varphi(x_U)^{p^2}\varphi(N_U(x_U))\nu_{\mathcal{L},U}(x_{C_n})}\right)\right)+Tr_{U/Z_m\cap U}\left(\mu_{\mathcal{L},U}(x_U)\sum_{\beta\in(\mathbb{Z}/p^i\mathbb{Z})^\times} rc_{1,\beta}^{n-i}\right)$
  $= \frac{1}{p}log\left(Nm_{C_n/Z_m\cap C_n}\left(\frac{x_{C_n}^p N_{C_n}(\varphi(x_{C_n}))^p\lambda_{\mathcal{L},C_n}((x_V))}{\varphi(x_{C_n})^p\varphi(N_{C_n}(x_{C_n}))}\right)\right)$ *for* $U \in \{N_{t^i}, N_{k^i}\}$ *and* $m \geq n-i$

*4. For any* $(x_V)_{V\in\mathcal{F}_n} \in \Theta_{n,R}$*, we have:*

- $Nm_{C_n/Z_m\cap C_n}\left(x_{C_n}^p N_{C_n}(\varphi(x_{C_n}))^p\left(\lambda_{\mathcal{L},C_n}((x_V)_{V\in\mathcal{F}_n})\right)\right)$
  $\equiv Nm_{C_n/Z_m\cap C_n}\left(\varphi(x_{C_n})^p\varphi\left(N_{C_n}(x_{C_n})\right)\right)$ $(mod\ p^{3m+1})$
- $Nm_{U/Z_m\cap U}\left(x_U^p N_U(\varphi(x_U))\left(\lambda_{\mathcal{L},U}((x_V)_{V\in\mathcal{F}_n})\right)\right)$
  $\equiv Nm_{U/Z_m\cap U}\left(\varphi(x_U)\varphi(N_U(x_U))\right)$ $(mod\ p^{3m})$ *for* $U \in \{T_n, K_n\}$
- $Nm_{U/Z_m\cap U}\left(x_U^p\varphi(N_U(x_U))^{p^2}\left(\lambda_{\mathcal{L},U}((x_V)_{V\in\mathcal{F}_n})\right)\right)$
  $\equiv Nm_{U/Z_m\cap U}\left(\varphi(x_U)^{p^2}\varphi(N_U(x_U))\left(\nu_{\mathcal{L},U}(x_{C_n})\right)\right)$ $(mod\ p^{3m+1})$ *for* $U \in \{N_{t^i}, N_{k^i}\}$

**Theorem 5.1** *The image of* $\theta_n$ *is contained in* $\Theta_{n,\mathbb{Z}_p}$.

**Proof:**
We prove this theorem by proving each individual condition of $\Psi_{n,\mathbb{Z}_p}$ is satisfied in the image of $\Theta_{n,\mathbb{Z}_p}$ under the map $\mathcal{L}$. We start with conditions 2 and 3. Recall condition 2 and 3 from the definition of $\Psi_{n,\mathbb{Z}_p}$:

2. For any $(a_V)_{V\in\mathcal{F}_n} \in \Psi_{n,\mathbb{Z}_p}$, each $a_V$ is fixed by conjugation action of $N_{G_n}(V)$
3. For any $(a_V)_{V\in\mathcal{F}_n} \in \Psi_{n,\mathbb{Z}_p}$, we have:

- $Tr_{V/Z_n}(a_V) = a_{Z_n}$ for all $V \in \mathcal{F}_n$
- $Tr_{N_{t^i}/Z_m\cap N_{t^i}}(a_{N_{t^i}}) = Tr_{C_n/Z_m\cap C_n}(a_{C_n})$ for $m \geq n-i$
- $Tr_{N_{k^i}/Z_m\cap N_{k^i}}(a_{N_{k^i}}) = Tr_{C_n/Z_m\cap C_n}(a_{C_n})$ for $m \geq n-i$

Due to the properties of logarithm and the definitions of norm[4]and trace, these conditions are clearly satisfied in the image of $\mathcal{L}$ by the respective conditions 2 and 3 from $\Theta_{n,\mathbb{Z}_p}$.
Now we prove condition 1. Condition 1 in the definition of $\Psi_{n,\mathbb{Z}_p}$ says this:

$$1.\Psi_{n,\mathbb{Z}_p} \subset p^{3n-2}\mathbb{Z}_p[Z_n]\times\mathbb{Z}_p[C_n]\times\mathbb{Z}_p[T_n]\times\mathbb{Z}_p[K_n]\times\prod_{i=1}^{n-1}\left(\mathbb{Z}_p[N_{t^i}]\times\mathbb{Z}_p[N_{k^i}]\right)$$

This is equivalent to the condition $\forall(a_V)_{V\in\mathcal{F}_n} \in \Psi_{n,\mathbb{Z}_p}$ we have $(a_V)_{V\in\mathcal{F}_n} \in \prod_{U\in\mathcal{F}_n}\mathbb{Z}_p[U]$ such that $p^{3n-2}|a_{Z_n}$. Now we replace $a_U$ with $\mathcal{L}_U((x_V)_{V\in\mathcal{F}_n})$. By definition of $\mathcal{L}$ this condition is equivalent[5]to:

$$p^{3n-2}\left|\frac{1}{p}log\left(\frac{x_{Z_n}^p\lambda_{\mathcal{L},Z_n}((x_V))}{\varphi(x_{Z_n})}\right)\right.$$

By the properties of logarithm, one can see that these conditions are equivalent to condition 1 of $\Theta_{n,\mathbb{Z}_p}$.

[4]Let V be a group and U a subgroup of V. For any $A \in V$ the norm is defined in the following way:

$$Nm_{V/U}(A) := \prod_{\substack{X\in U\setminus V\\ X^{-1}AX\in U}} X^{-1}AX$$

[5]At this point we are not concerned with proving $\mathcal{L}((x_V)) \in \prod_{U\in\mathcal{F}_n}\mathbb{Z}_p[U]$, we want to prove that image of $\theta_n$ is contained in $\Theta_{n,\mathbb{Z}_p}$ so we are satisfied with $\mathcal{L}((x_V)) \in \prod_{U\in\mathcal{F}_n}\mathbb{Q}_p\otimes_{\mathbb{Z}_p}\mathbb{Z}_p[U]$

Finally, we prove condition 4. Condition 4 from the definition of $\Psi_{n,\mathbb{Z}_p}$ states:

4. For any $(a_V)_{V\in\mathcal{F}_n} \in \Psi_{n,\mathbb{Z}_p}$, we have:

- $Tr_{C_n/Z_m\cap C_n}(a_{C_n}) \in p^{3m}\mathbb{Z}_p[C_n]$
- $Tr_{T_n/Z_m\cap T_n}(a_{T_n}) \in p^{3m-1}\mathbb{Z}_p[T_n]$
- $Tr_{K_n/Z_m\cap K_n}(a_{K_n}) \in p^{3m-1}\mathbb{Z}_p[K_n]$
- $Tr_{N_{t^i}/Z_m\cap N_{t^i}}(a_{N_{t^i}}) \in p^{3m}\mathbb{Z}_p[N_{t^i}]$
- $Tr_{N_{k^i}/Z_m\cap N_{k^i}}(a_{N_{k^i}}) \in p^{3m}\mathbb{Z}_p[N_{k^i}]$

We rewrite these conditions in the form $p^{3m}|Tr_{C_n/Z_m\cap C_n}(a_{C_n})$, $p^{3m-1}|Tr_{T_n/Z_m\cap T_n}(a_{T_n})$, $p^{3m-1}|Tr_{K_n/Z_m\cap K_n}(a_{K_n})$, $p^{3m}|Tr_{N_{t^i}/Z_m\cap N_{t^i}}(a_{N_{t^i}})$ and $p^{3m}|Tr_{N_{k^i}/Z_m\cap N_{k^i}}(a_{N_{k^i}})$.
Recall the definition of $\mu_{f,N}(a_N) =$

$$\frac{p}{2}\varphi\left(\frac{Tr_{N/(Z_{n-i-1}\cap N)}(a_N)}{[N : Z_{n-i-1}\cap N]} - \frac{Tr_{N/(Z_{n-i}\cap N)}(a_N)}{[N : Z_{n-i}\cap N]}\right)$$

for $N \in \{N_{t^i}, N_{k^i} | i = 1, ..., n-1\}$.
By condition 4 from the definition of $\Psi_{n,\mathbb{Z}_p}$, we know that $p^{3m}|Tr_{N/(Z_m\cap N)}(a_N)$, but we also have $[N : Z_m \cap N] = p^m$, therefore $p^{2(n-i)+1}|\mu_{f,N}(a_N)$.
Recall that $\mu_{\mathcal{L},N} \in \mathbb{Q}_p^\times \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[Z_{n-i}\cap C_n]^\times$, thus $\mu_{\mathcal{L},N}$ will have the form:

$$\mu_{\mathcal{L},N} = \sum_{j\geq n-i}\sum_{x,\beta} a_{x,\beta,j} rc_{x,\beta}^j$$

where $a_{x,\beta,j} \in p^{2j+1}\mathbb{Z}_p^\times$. Therefore we have:

$$\mu_{f,N}(a_N)\sum_\beta rc_{1,\beta}^{n-i} = \sum_{j\geq n-i}\sum_{x,\beta} a_{x,\beta,j} rc_{x,\beta}^j$$

But we also know that

$$Tr_{C_n/Z_m\cap C_n}\left(rc_{x,\beta}^j\right) = \begin{cases} p^m rc_{x,\beta}^j & \text{if } j \geq m \\ 0 & \text{otherwise} \end{cases}$$

Therefore we can conclude that $p^{3m+1}|Tr_{C_n/Z_m\cap C_n}\left(\sum_{N=N_{t^i},N_{k^i}} \mu_{f,N}(a_N)\sum_\beta rc_{1,\beta}^{n-i}\right)$.
Recall that $\mathcal{L}_{C_n} = f_{C_n} \circ log$, so we have $Tr_{C_n/Z_m\cap C_n}(a_{C_n}) = Tr_{C_n/Z_m\cap C_n}(f_{C_n} \circ log(x_{C_n}))$. Let $log(x_{C_n}) = b_{C_n}$ then we have:

$$\begin{aligned} &Tr_{C_n/Z_m\cap C_n}(f_{C_n}(b_{C_n})) = \\ &\quad Tr_{C_n/Z_m\cap C_n}\Big(b_{C_n} - \varphi(b_{C_n}) - \tfrac{1}{p}\varphi\left(T_{C_n}(b_{C_n})\right) + T_{C_n}(\varphi(b_{C_n})) - [G_n : C_n]\lambda_f((b_V)) \\ &\quad - \sum_{N=N_{t^i},N_{k^i}} \mu_{f,N}(b_N)\sum_\beta rc_{1,\beta}^{n-i}\Big) \\ &= \quad Tr_{C_n/Z_m\cap C_n}\Big(b_{C_n} - \varphi(b_{C_n}) - \tfrac{1}{p}\varphi\left(T_{C_n}(b_{C_n})\right) + T_{C_n}(\varphi(b_{C_n})) - [G_n : C_n]\lambda_f((b_V))\Big) \\ &\quad -Tr_{C_n/Z_m\cap C_n}\Big(\sum_{N=N_{t^i},N_{k^i}} \mu_{f,N}(b_N)\sum_\beta rc_{1,\beta}^{n-i}\Big) \end{aligned}$$

This means that the condition $p^{3m}|Tr_{C_n/Z_m\cap C_n}(a_{C_n})$ implies that we need

$$p^{3m}|Tr_{C_n/Z_m\cap C_n}\Big(b_{C_n} - \varphi(b_{C_n}) - \frac{1}{p}\varphi\left(T_{C_n}(b_{C_n})\right) + T_{C_n}(\varphi(b_{C_n})) - [G_n : C_n]\lambda_f((b_V))\Big)$$

By the same reasoning, we also find that the conditions $p^{3m}|Tr_{N_{t^i}/Z_m\cap N_{t^i}}(a_{N_{t^i}})$ and $p^{3m}|Tr_{N_{k^i}/Z_m\cap N_{k^i}}(a_{N_{k^i}})$ imply that we need:

$$p^{3m}|Tr_{U/Z_m\cap U}\Big(b_U - p\varphi(b_U) - \frac{1}{p}\varphi\left(T_U(b_U)\right) + p\varphi\left(T_U(b_U)\right) - [G_n : U]\lambda_f((b_V)) + \nu_{f,U}(b_{C_n})\Big)$$

for $U = N_{t^i}$ or $N_{k^i}$

Now we can rewrite these five conditions in the following forms:

$$p^{3m}\Big|Tr_{C_n/Z_m\cap C_n}\left(\frac{1}{p}log\left(\frac{x_{C_n}^p N_{C_n}(\varphi(x_{C_n}))^p\lambda_{\mathcal{L},C_n}((x_V))}{\varphi(x_{C_n})^p\varphi\left(N_{C_n}(x_{C_n})\right)}\right)\right)$$

$$p^{3m-1}\Big|Tr_{T_n/Z_m\cap T_n}\left(\frac{1}{p}log\left(\frac{x_{T_n}^p N_{T_n}(\varphi(x_{T_n}))\lambda_{\mathcal{L},T_n}((x_V))}{\varphi(x_{T_n})\varphi(N_{T_n}(x_{T_n}))}\right)\right)$$

$$p^{3m-1}\Big|Tr_{K_n/Z_m\cap K_n}\left(\frac{1}{p}log\left(\frac{x_{K_n}^p N_{K_n}(\varphi(x_{K_n}))\lambda_{\mathcal{L},K_n}((x_V))}{\varphi(x_{K_n})\varphi(N_{K_n}(x_{K_n}))}\right)\right)$$

$$p^{3m}\Big|Tr_{N_{t^i}/Z_m\cap N_{t^i}}\left(\frac{1}{p}log\left(\frac{x_{N_{t^i}}^p\varphi(N_{N_{t^i}}(x_{N_{t^i}}))^{p^2}\lambda_{\mathcal{L},N_{t^i}}((x_V))}{\varphi(x_{N_{t^i}})^{p^2}\varphi(N_{N_{t^i}}(x_{N_{t^i}}))\nu_{\mathcal{L},N_{t^i}}(x_{C_n})}\right)\right)$$

$$p^{3m}\Big|Tr_{N_{k^i}/Z_m\cap N_{k^i}}\left(\frac{1}{p}log\left(\frac{x_{N_{k^i}}^p\varphi(N_{N_{k^i}}(x_{N_{k^i}}))^{p^2}\lambda_{\mathcal{L},N_{k^i}}((x_V))}{\varphi(x_{N_{k^i}})^{p^2}\varphi(N_{N_{k^i}}(x_{N_{k^i}}))\nu_{\mathcal{L},N_{k^i}}(x_{C_n})}\right)\right)$$

Like before, by the properties of logarithm one can see that these conditions are equivalent to condition 4 in $\Theta_{n,\mathbb{Z}_p}$ and thus the theorem is proved.

□

# Chapter 6

# Whitehead group of the localised algebra $\widehat{\widetilde{\Lambda(G_n)}_{\mathcal{T}'}}$

In this chapter we will modify the work done in this paper to prove that $\widetilde{\theta_n}\left(K_1\left(\widehat{\Lambda(\widetilde{G_n})_{\mathcal{T}'}}\right)\right)$ lies in the group $\Theta^{\tau}_{n,\widehat{\mathbb{Z}_p[[\Gamma_n]]_{(p)}}}$ which is defined below. Recall the isomorphism from lemma 2.4:

$$\widehat{\mathbb{Z}_p[[\Gamma_n]]}_T[G_n]^{\tau} \cong \widehat{\Lambda(\widetilde{G_n})}_{\mathcal{T}'}$$

where $T = \mathbb{Z}_p[[\Gamma_n]] - p\mathbb{Z}_p[[\Gamma_n]]$. But $\widehat{\mathbb{Z}_p[[\Gamma_n]]}$ has inverse elements for all elements in $T$ except for powers of $p$, therefore $\widehat{\mathbb{Z}_p[[\Gamma_n]]}_T \cong \widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}$.
We expect to have the following commutative diagram:

$$\begin{array}{ccccccc} ker(Log) & \to & K_1\left(\widehat{\Lambda(\widetilde{G_n})_{\mathcal{T}'}}\right) & \xrightarrow{Log} & \widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}[Conj(G_n)]^{\tau} & \to & coker(Log) \\ & & \downarrow \widetilde{\theta_n} & & \downarrow \widetilde{\psi_n} & & \\ ker(\mathcal{L}) & \to & \Theta^{\tau}_{n,\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}} & \xrightarrow{\mathcal{L}} & \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \Psi^{\tau}_{n,\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}} & \to & coker(\mathcal{L}) \end{array}$$

where $\Theta^{\tau}_{n,R}$ and $\Psi^{\tau}_{n,R}$ is the notation used to denote the analogue to $\Theta_{n,R}$ and $\Psi_{n,R}$ which use twisted group rings[1]. Also $\widetilde{\theta_n}$ and $\widetilde{\psi_n}$ are the analogue maps of $\theta_n$ and $\psi_n$ respectively. If this diagram commutes then we have proved that $\widetilde{\theta_n}\left(K_1\left(\widehat{\Lambda(\widetilde{G_n})_{\mathcal{T}'}}\right)\right)$ is contained in $\Theta^{\tau}_{n,\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}}$.
This is very similar to the work we have already done in this paper so we only need to verify that the twist does not change the image of the maps and that the maps $\mathcal{L}$ and $Log$ are still well-defined on $\Theta^{\tau}_{n,\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}}$ and $K_1\left(\widehat{\Lambda(\widetilde{G_n})_{\mathcal{T}'}}\right)$ respectively. We need to check this is because both $\mathcal{L}$ and $Log$ are defined using logarithm.

## 6.1 Inspecting the twist $\tau$

This section is focused on the map $\widetilde{\psi_n}$ and understanding the module[2] $\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}[Conj(G_n)]^{\tau}$.
Let $A, X \in G_n$, then their images in $\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}[G_n]^{\tau}$ are $\overline{A}$ and $\overline{X}$ respectively. Recall that, for elements in $G_n$, multiplication in $\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}[G_n]^{\tau}$ has the twist

$$\overline{A} \cdot \overline{X} = \tau(A, X)\overline{AX}$$

[1] $\Psi^{\tau}_{n,R}$ and $\Theta^{\tau}_{n,R}$ have the same definitions as $\Psi_{n,R}$ and $\Theta_{n,R}$ except that instead of $\Psi_{n,R} \subset \prod_{U\in\mathcal{F}_n} R[U]$ and $\Theta_{n,R} \subset \prod_{U\in\mathcal{F}_n} R[U]^{\times}$ we have $\Psi^{\tau}_{n,R} \subset \prod_{U\in\mathcal{F}_n} R[U]^{\tau}$ and $\Theta^{\tau}_{n,R} \subset \prod_{U\in\mathcal{F}_n} (R[U]^{\tau})^{\times}$.

[2] $R[Conj(G)]^{\tau}$ is the $R$-module over the basis of all conjugacy classes of $G$ in the twisted group ring $R[G]^{\tau}$ i.e. two elements $g$ and $h$ in $G$ are conjugate in $R[G]^{\tau}$ if there exists $x \in G$ such that $\overline{g} = \overline{x}^{-1} \cdot \overline{h} \cdot \overline{x}$.

**Lemma 6.1** *For any $A, X \in G_n$, we have $\overline{X}^{-1} \cdot \overline{A} \cdot \overline{X} = \overline{X^{-1}AX}$ in $[G_n]^\tau$*

*Proof:*

$$\overline{X}^{-1} \cdot \overline{A} \cdot \overline{X} = \tau(X^{-1}, A)\overline{X^{-1}A} \cdot \overline{X} = \tau(X^{-1}, A)\tau(X^{-1}A, X)\overline{X^{-1}AX}$$

So we just need to prove that $\tau(X^{-1}, A)\tau(X^{-1}A, X) = \mathbf{1}_2$
The 2-cocycle, $\tau$, has the following properties $\tau(A, A^{-1}) = \mathbf{1}_2 = \tau(A, \mathbf{1}_2)$ and $\tau(A, B) = \tau(B, A)$ (see lemma 2.1).
By definition of 2-cocycle we know that

$$\tau(B, A)\tau(BA, X) = \left(\overline{B} * \tau(A, X)\right)\tau(B, AX)$$

where $*$ denotes conjugation. But $\tau(A, X) \in \Gamma_n$ so $\tau(A, X)$ is in the centre of $\widetilde{G_n}$, therefore $\overline{B} * \tau(A, X) = \tau(A, X)$

$$\begin{aligned}
\tau(X^{-1}, A)\tau(X^{-1}A, X) &= \left(\overline{X^{-1}} * \tau(A, X)\right)\tau(X^{-1}, AX) \\
&= \tau(A, X)\tau(X^{-1}, AX) \\
&= \tau(A, X)\tau(AX, X^{-1}) \\
&= \left(\overline{A} * \tau(X, X^{-1})\right)\tau(A, XX^{-1}) \\
&= \mathbf{1}_2 \cdot \tau(A, \mathbf{1}_2) \\
&= \mathbf{1}_2
\end{aligned}$$

□

With this lemma, we know that the conjugacy class basis of $\widehat{\mathbb{Z}_p[[\Gamma_n]]_{(p)}}[Conj(G_n)]^\tau$ have a one-to-one correspondence with the basis of $\mathbb{Z}_p[Conj(G_n)]$. We also know that $\widetilde{\psi_n}$ acts on $\widehat{\mathbb{Z}_p[[\Gamma_n]]_{(p)}}[Conj(G_n)]^\tau$ in same that $\psi_n$ acts on $\mathbb{Z}_p[Conj(G_n)]$, thus the image of $\widetilde{\psi_n}$ is in fact $\Psi^\tau_{n,\widehat{\mathbb{Z}_p[[\Gamma_n]]_{(p)}}}$.

## 6.2 Verifying that we can take *log*

This section will focus on the maps *Log* and $\mathcal{L}$.
By ([11], Section 5.5.2), we know that *Log* is well defined on $K_1\left(\Lambda(\widehat{\widetilde{G_n}})_{\mathcal{T}'}\right)$. Also due to ([11], Section 5.5.2), we only need to show that $\mathcal{L}$ is well defined on $\widehat{\mathbb{Z}_p[[\Gamma_n]]_{(p)}}$ in order to prove that $\mathcal{L}$ is well defined on $\Theta^\tau_{n,\widehat{\mathbb{Z}_p[[\Gamma_n]]_{(p)}}}$.

Recall the definition of $\mathcal{L}$:

$\mathcal{L} = \prod_{U \in \mathcal{F}} \mathcal{L}_U$ such that

$$\mathcal{L}_U((x_V)) := \begin{cases} \frac{1}{p} log \left( \frac{x_U^p \varphi(N_U(x_U))^{p^2} \lambda_{\mathcal{L},U}((x_V))}{\varphi(x_U)^{p^2} \varphi(N_U(x_U)) \nu_{\mathcal{L},U}(x_{C_n})} \right) & \\ - \sum_{\substack{N = N_{tl}, N_{kl} \\ l \leq i}} \mu_{\mathcal{L},N}(x_N) \sum_{\beta \in (\mathbb{Z}/p^i\mathbb{Z})^\times} rc_{1,\beta}^{n-l} & \\ + \mu_{\mathcal{L},U}(x_U) \sum_{\beta \in (\mathbb{Z}/p^i\mathbb{Z})^\times} rc_{1,\beta}^{n-i} & \text{if } U = N_{t^i} \text{ or } N_{k^i} \\ \\ \frac{1}{p} log \left( \frac{x_{C_n}^p N_{C_n}(\varphi(x_{C_n}))^p \lambda_{\mathcal{L},C_n}((x_V))}{\varphi(x_{C_n})^p \varphi\big(N_{C_n}(x_{C_n})\big)} \right) & \\ - \sum_{N = N_{t^i}, N_{k^i}} \mu_{\mathcal{L},N}(x_N) \sum_{\beta \in (\mathbb{Z}/p^i\mathbb{Z})^\times} rc_{1,\beta}^{n-i} & \text{if } U = C_n \\ \\ \frac{1}{p} log \left( \frac{x_{Z_n}^p \lambda_{\mathcal{L},Z_n}((x_V))}{\varphi(x_{Z_n})} \right) & \text{if } U = Z_n \\ \\ \frac{1}{p} log \left( \frac{x_U^p N_U(\varphi(x_U)) \lambda_{\mathcal{L},U}((x_V))}{\varphi(x_U) \varphi(N_U(x_U))} \right) & \text{if } U = T_n \text{ or } K_n \end{cases}$$

where $N_U(x_U) = Nm_{U/Z_n}(x_U)^{\frac{1}{[U:Z_n]}}$, $\lambda_{\mathcal{L},U}$ is a map from $\prod_{U \in \mathcal{F}_n} \mathbb{Z}_p[U]^\times$ to $\mathbb{Q}_p^\times \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[Z_n]^\times$, $\mu_{\mathcal{L},N}$ is a map from $\mathbb{Z}_p[N]^\times$ to $\mathbb{Q}_p^\times \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[Z_{n-i} \cap C_n]^\times$ and $\nu_{\mathcal{L},N}$ is a map from $\mathbb{Z}_p[C_n]^\times$ to $\mathbb{Q}_p^\times \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[N]^\times$ for $N \in \{N_{t^i}, N_{k^i} | i = 1, 2, ..., n-1\}$. These maps are defined in the following way:

$$\lambda_{\mathcal{L},U}((x_V)) = \prod_{W = C_n, T_n, K_n} Nm_{W/Z_n} \left( \frac{\varphi(Nm_{W/Z_n}(x_W))}{\varphi(x_W)^{[W:Z_n]}} \right)^{\frac{[G_n:U]}{[W:Z_n]^2}}$$

$$\mu_{\mathcal{L},N}(x_N) = log \left( \varphi \left( \frac{Nm_{N/(Z_{n-i-1} \cap N)}(x_N)^p}{Nm_{N/(Z_{n-i} \cap N)}(x_N)} \right)^{\frac{p}{2[N:Z_{n-i} \cap N]}} \right)$$

$$\nu_{\mathcal{L},N}(x_{C_n}) = Nm_{C_n/(Z_{n-i} \cap C_n)} \left( \frac{N_{C_n}(x_{C_n}) \varphi(x_{C_n})}{x_{C_n} N_{C_n}(\varphi(x_{C_n}))} \right)^p$$

Also recall the definition of $\Theta^\tau_{n, \widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}}$:

1. $\Theta_{n, \widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}} \subset \prod_{U \in \mathcal{F}_n} (\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}[U]^\tau)^\times$ such that $x_{Z_n}^p \left( \lambda_{\mathcal{L},Z_n}((x_V)_{V \in \mathcal{F}_n}) \right) \equiv \varphi(x_{Z_n}) \ (mod\ p^{3n-1})$
2. For any $(x_V)_{V \in \mathcal{F}_n} \in \Theta_{n, \widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}}$, each $x_V$ is fixed by conjugation action of $N_{G_n}(V)$
3. For any $(x_V)_{V \in \mathcal{F}_n} \in \Theta_{n, \widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}}$, we have:
   - $Nm_{V/Z_n}(x_V) = x_{Z_n}$ for all $V \in \mathcal{F}_n$
   - $\frac{1}{p} log \left( Nm_{U/Z_m \cap U} \left( \frac{x_U^p \varphi(N_U(x_U))^{p^2} \lambda_{\mathcal{L},U}((x_V))}{\varphi(x_U)^{p^2} \varphi(N_U(x_U)) \nu_{\mathcal{L},U}(x_{C_n})} \right) \right) + Tr_{U/Z_m \cap U} \left( \mu_{\mathcal{L},U}(x_U) \sum_{\beta \in (\mathbb{Z}/p^i\mathbb{Z})^\times} rc_{1,\beta}^{n-i} \right)$
     $= \frac{1}{p} log \left( Nm_{C_n/Z_m \cap C_n} \left( \frac{x_{C_n}^p N_{C_n}(\varphi(x_{C_n}))^p \lambda_{\mathcal{L},C_n}((x_V))}{\varphi(x_{C_n})^p \varphi\big(N_{C_n}(x_{C_n})\big)} \right) \right)$ for $U \in \{N_{t^i}, N_{k^i}\}$ and $m \geq n - i$
4. For any $(x_V)_{V \in \mathcal{F}_n} \in \Theta_{n, \widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}}$, we have:
   - $Nm_{C_n/Z_m \cap C_n} \left( x_{C_n}^p N_{C_n}(\varphi(x_{C_n}))^p \left( \lambda_{\mathcal{L},C_n}((x_V)_{V \in \mathcal{F}_n}) \right) \right)$
     $\equiv Nm_{C_n/Z_m \cap C_n} \left( \varphi(x_{C_n})^p \varphi\left(N_{C_n}(x_{C_n})\right) \right) \ (mod\ p^{3m+1})$

- $Nm_{U/Z_m\cap U}\left(x_U^p N_U(\varphi(x_U))\left(\lambda_{\mathcal{L},U}((x_V)_{V\in\mathcal{F}_n})\right)\right)$
  $\equiv Nm_{U/Z_m\cap U}\left(\varphi(x_U)\varphi(N_U(x_U))\right)\ (mod\ p^{3m})$ for $U\in\{T_n,K_n\}$
- $Nm_{U/Z_m\cap U}\left(x_U^p\varphi(N_U(x_U))^{p^2}\left(\lambda_{\mathcal{L},U}((x_V)_{V\in\mathcal{F}_n})\right)\right)$
  $\equiv Nm_{U/Z_m\cap U}\left(\varphi(x_U)^{p^2}\varphi(N_U(x_U))\left(\nu_{\mathcal{L},U}(x_{C_n})\right)\right)\ (mod\ p^{3m+1})$ for $U\in\{N_{t^i},N_{k^i}\}$

**Lemma 6.2** *$\mathcal{L}$ is well defined on $\Theta^{\tau}_{n,\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}}$*

*Proof:*
As mentioned above, we will only show that $\mathcal{L}$ is well defined on $\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}$.
The logarithm is only defined on elements in the form $1+py$ where $y\in\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}$. By inspecting $\mathcal{L}$, we see that we need to prove the following

$$\frac{x_{Z_n}^p\lambda_{\mathcal{L},Z_n}((x_V))}{\varphi(x_{Z_n})}\equiv 1\ (mod\ p)\qquad\text{if } U=Z_n$$

$$\frac{x_U^p N_U(\varphi(x_U))\lambda_{\mathcal{L},U}((x_V))}{\varphi(x_U)\varphi(N_U(x_U))}\equiv 1\ (mod\ p)\quad\text{if } U=T_n \text{ or } K_n$$

In fact, the condition for $U=Z_n$ is already satisfied by condition 1 of $\Theta^{\tau}_{n,\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}}$.
We have left out the cases when $U=C_n,N_{t^i}$ or $N_{k^i}$ for now because first we want to inspect $\mu_{\mathcal{L},N}(x_N)$. We can rearrange the second bullet point of condition 3 of the definition of $\Theta^{\tau}_{n,\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}}$ to get the following:
$Tr_{U/Z_m\cap U}\left(\mu_{\mathcal{L},U}(x_U)\sum_{\beta\in(\mathbb{Z}/p^i\mathbb{Z})^\times}rc_{1,\beta}^{n-i}\right)=$
$\frac{1}{p}log\left(Nm_{C_n/Z_m\cap C_n}\left(\frac{x_{C_n}^p N_{C_n}(\varphi(x_{C_n}))^p\lambda_{\mathcal{L},C_n}((x_V))}{\varphi(x_{C_n})^p\varphi\left(N_{C_n}(x_{C_n})\right)}\right)\right)-\frac{1}{p}log\left(Nm_{U/Z_m\cap U}\left(\frac{x_U^p\varphi(N_U(x_U))^{p^2}\lambda_{\mathcal{L},U}((x_V))}{\varphi(x_U)^{p^2}\varphi(N_U(x_U))\nu_{\mathcal{L},U}(x_{C_n})}\right)\right)$
for $U\in\{N_{t^i},N_{k^i}\}$ and $m\geq n-i$. But by condition 4 of $\Theta^{\tau}_{n,\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}}$ we know that the RHS belongs to $p^{3m}\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}$.
Also, if we take $m=n-i$ then we get:

$$Tr_{U/Z_{n-i}\cap U}\left(\mu_{\mathcal{L},U}(x_U)\sum_{\beta\in(\mathbb{Z}/p^i\mathbb{Z})^\times}rc_{1,\beta}^{n-i}\right)=p^{n-i}\mu_{\mathcal{L},U}(x_U)\sum_{\beta\in(\mathbb{Z}/p^i\mathbb{Z})^\times}rc_{1,\beta}^{n-i}$$

Thus we can conclude that $\mu_{\mathcal{L},N}(x_N)$ is divisible by $p^{2(n-i)}$.
So for $U=C_n,N_{t^i}$ or $N_{k^i}$ we need to prove the following

$$\frac{x_U^p\varphi(N_U(x_U))^{p^2}\lambda_{\mathcal{L},U}((x_V))}{\varphi(x_U)^{p^2}\varphi(N_U(x_U))\nu_{\mathcal{L},U}(x_{C_n})}\equiv 1\ (mod\ p)\qquad\text{if } U=N_{t^i}\text{ or }N_{k^i}$$

$$\frac{x_{C_n}^p N_{C_n}(\varphi(x_{C_n}))^p\lambda_{\mathcal{L},C_n}((x_V))}{\varphi(x_{C_n})^p\varphi\left(N_{C_n}(x_{C_n})\right)}\equiv 1\ (mod\ p)\quad\text{if } U=C_n$$

Let us inspect $\lambda_{\mathcal{L},U}((x_V))$:

$$\lambda_{\mathcal{L},U}((x_V))=\prod_{W=C_n,T_n,K_n}Nm_{W/Z_n}\left(\frac{\varphi(Nm_{W/Z_n}(x_W))}{\varphi(x_W)^{[W:Z_n]}}\right)^{\frac{[G_n:U]}{[W:Z_n]^2}}$$

By condition 3 of $\Theta^{\tau}_{n,\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}}$ we know that $Nm_{W/Z_n}(x_W) = x_Z$, so we have

$$\begin{aligned}
\lambda_{\mathcal{L},U}((x_V)) &= \prod_{W=C_n,T_n,K_n} Nm_{W/Z_n}\left(\frac{\varphi(x_Z)}{\varphi(x_W)^{[W:Z_n]}}\right)^{\frac{[G_n:U]}{[W:Z_n]^2}} \\
&= \prod_{W=C_n,T_n,K_n}\left(\frac{Nm_{W/Z_n}(\varphi(x_Z))}{Nm_{W/Z_n}(\varphi(x_W)^{[W:Z_n]})}\right)^{\frac{[G_n:U]}{[W:Z_n]^2}} \\
&= \prod_{W=C_n,T_n,K_n}\left(\frac{\varphi(x_Z)}{Nm_{W/Z_n}(\varphi(x_W))}\right)^{\frac{[G_n:U]}{[W:Z_n]}}
\end{aligned}$$

We know that $\varphi(x_W) \equiv x_W^p (mod\ p)$, therefore $Nm_{W/Z_n}(\varphi(x_W)) \equiv Nm_{W/Z_n}(x_W)^p\ (mod\ p)$ and then we can use condition 3 of $\Theta^{\tau}_{n,\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}}$ again

$$\lambda_{\mathcal{L},U}((x_V)) \equiv \prod_{W=C_n,T_n,K_n}\left(\frac{x_Z^p}{x_Z^p}\right)^{\frac{[G_n:U]}{[W:Z_n]}} \equiv 1\ (mod\ p)$$

So for the cases $U = T_n$ or $K_n$, we need

$$\frac{x_U^p N_U(\varphi(x_U))}{\varphi(x_U)\varphi(N_U(x_U))} \equiv 1\ (mod\ p)$$

But this is clearly satisfied since $\varphi(x_U) \equiv x_U^p\ (mod\ p)$.
Now we will check the case $U = C_n$. Condition 4 of $\Theta^{\tau}_{n,\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}}$ tells us

$$\begin{aligned}
&Nm_{C_n/Z_m\cap C_n}\left(x_{C_n}^p N_{C_n}(\varphi(x_{C_n}))^p\left(\lambda_{\mathcal{L},C_n}((x_V)_{V\in\mathcal{F}_n})\right)\right) \\
&\equiv Nm_{C_n/Z_m\cap C_n}\left(\varphi(x_{C_n})^p\varphi\left(N_{C_n}(x_{C_n})\right)\right)\ (mod\ p^{3m+1})
\end{aligned}$$

But $\varphi(x_{C_n}) \in Z_1 \cap C_n$ (see proof of Proposition 5.1) and $N_{C_n}(x_{C_n}) \in Z_n \subset Z_1 \cap C_n$, thus we get

$$\begin{aligned}
& Nm_{C_n/Z_1\cap C_n}\left(x_{C_n}^p N_{C_n}(\varphi(x_{C_n}))^p(\lambda_{\mathcal{L},C_n}((x_V)_{V\in\mathcal{F}_n}))\right) \\
& \equiv (\varphi(x_{C_n})^p\varphi(N_{C_n}(x_{C_n})))^{[C_n:Z_1\cap C_n]}\ (mod\, p) \\
\iff\ & Nm_{C_n/Z_1\cap C_n}\left(\varphi(x_{C_n})N_{C_n}(\varphi(x_{C_n}))^p\right) \equiv (\varphi(x_{C_n})^p\varphi(N_{C_n}(x_{C_n})))^{[C_n:Z_1\cap C_n]}\ (mod\ p) \\
\iff\ & (\varphi(x_{C_n})N_{C_n}(\varphi(x_{C_n}))^p)^{[C_n:Z_1\cap C_n]} \equiv (\varphi(x_{C_n})^p\varphi(N_{C_n}(x_{C_n})))^{[C_n:Z_1\cap C_n]}\ (mod\ p) \\
\iff\ & \left(\frac{\varphi(x_{C_n})N_{C_n}(\varphi(x_{C_n}))^p}{\varphi(x_{C_n})^p\varphi(N_{C_n}(x_{C_n}))}\right)^{[C_n:Z_1\cap C_n]} \equiv 1\ (mod\ p) \\
\iff\ & \left(\frac{x_{C_n}^p N_{C_n}(\varphi(x_{C_n}))^p\lambda_{\mathcal{L},C_n}((x_V)_{V\in\mathcal{F}_n})}{\varphi(x_{C_n})^p\varphi(N_{C_n}(x_{C_n}))}\right)^p \equiv 1\ (mod\ p)
\end{aligned}$$

The exact same method can be used for the cases $U = N_{t^i}$ or $N_{k^i}$:
We know that $\nu_{\mathcal{L},U}(x_{C_n}), \varphi(x_U) \in Z_1 \cap U$ and $N_U(x_U) \in Z_n \subset Z_1 \cap U$, so we just use condition 4 of $\Theta^{\tau}_{n,\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}}$:

$$\begin{aligned}
& Nm_{U/Z_1\cap U}\left(x_U^p\varphi(N_U(x_U))^{p^2}\right) \equiv \left(\varphi(x_U)^{p^2}\varphi(N_U(x_U))\left(\nu_{\mathcal{L},U}(x_{C_n})\right)\right)^{[U:Z_1\cap U]}\ (mod\ p) \\
\iff\ & \left(\varphi(x_U)\varphi(N_U(x_U))^{p^2}\right)^{[U:Z_1\cap U]} \equiv \left(\varphi(x_U)^{p^2}\varphi(N_U(x_U))\left(\nu_{\mathcal{L},U}(x_{C_n})\right)\right)^{[U:Z_1\cap U]}\ (mod\ p) \\
\iff\ & \left(\frac{\varphi(x_U)\varphi(N_U(x_U))^{p^2}}{\varphi(x_U)^{p^2}\varphi(N_U(x_U))\nu_{\mathcal{L},U}(x_{C_n})}\right)^{[U:Z_1\cap U]} \equiv 1\ (mod\ p) \\
\iff\ & \left(\frac{x_U^p\varphi(N_U(x_U))^{p^2}\lambda_{\mathcal{L},U}((x_V))}{\varphi(x_U)^{p^2}\varphi(N_U(x_U))\nu_{\mathcal{L},U}(x_{C_n})}\right)^p \equiv 1\ (mod\ p)
\end{aligned}$$

□

With that last lemma we have proved the following

**Theorem 6.1** *The image of* $K_1\left(\Lambda(\widehat{\widetilde{G_n}})_{\mathcal{T}'}\right)$ *under the map* $\widetilde{\theta_n}$ *is contained in* $\Theta^{\tau}_{n,\widehat{\mathbb{Z}_p[[\Gamma_n]]}_{(p)}}$.

# Bibliography


[1] N. Bourbaki. *Commutative Algebra*. Hermann, Paris, 1965.

[2] D. Burns and O. Venjakob. On descent theory and main conjectures in non-commutative iwasawa theory. *Journal of the Institute of Mathematics of Jussieu*, 10(1):59118, 2011.

[3] I. Chen. Jacobians of modular curves associated to normalizers of cartan subgroups of level $p^n$. *C. R. Math. Acad. Sci. Paris*, 339:187–192, 2004.

[4] J. Coates, T. Fukaya, K. Kato, R. Sujatha, and O. Venjakob. The $GL_2$ Main Conjecture for Elliptic Curves without Complex Multiplication. *Publications mathématiques de l'IHÉS*, 101(1):163–208, 2005.

[5] J. Coates and S. Howson. Euler characteristics and elliptic curves ii. *J. Math. Soc. Japan*, 53(1):175–235, 01 2001.

[6] G. Ellis. The schur multiplier of a pair of groups. *Applied Categorical Structures*, 6(3):355–371, 1998.

[7] T. Fukaya and K. Kato. A formulation of conjectures on p-adic zeta functions in non-commutative iwasawa theory, preprint, 2003.

[8] T. Hara. Iwasawa theory of totally real fields for certain non-commutative $p$-extensions. *J. Number Theory*, 130:1068–1097, 2010.

[9] T. Hara. Inductive construction of the $p$ -adic zeta functions for noncommutative $p$ -extensions of exponent $p$ of totally real fields. *Duke Math. J.*, 158(2):247–305, 06 2011.

[10] M. Kakde. Proof of the Main Conjecture of Noncommutative Iwasawa Theory for Totally Real Number Fields in Certain Cases. *J. Algebraic Geometry*, 20:631–683, 2011.

[11] M. Kakde. The main conjecture of iwasawa theory for totally real fields. *Invent. Math*, 193:539–626, 2013.

[12] M. Kakde. Some congruences for non-cm elliptic curves. In D. Loeffler and S. Zerbes, editors, *Elliptic Curves, Modular Forms and Iwasawa Theory*, volume 188 of *Springer Proceedings in Mathematics & Statistics*. Springer International Publishing, 2015.

[13] K. Kato. Iwasawa theory of totally real fields for galois extensions of heisenberg type. preprint.

[14] R. Oliver. *Whitehead Groups of Finite Groups*. Cambridge University Press, 1988.

[15] J. Ritter and A. Weiss. On the "main conjecture" of equivariant iwasawa theory. *J. Amer. Math. Soc.*, 2011.

[16] K. Rubin. The main conjectures of iwasawa theory for imaginary quadratic fields. *Inventiones mathematicae*, 103(1):25–68, 1991.

[17] P. Schneider and O. Venjakob. K1 of certain iwasawa algebras, after kakde. 29, 10 2011.

[18] J.-P. Serre. Proprits galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15(4):259–331, 1971.

[19] R. Swan. *Algebraic K-Theory*. Springer, 1968.

[20] O. Venjakob. Characteristic elements in noncommutative Iwasawa theory. *J. reine angew. Math.*, 583:193–236, 2005.

[21] O. Venjakob. *On the Work of Ritter and Weiss in Comparison with Kakde's Approach*, pages 159–182. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[22] X. Wan. Introduction to Skinner-Urbans Work on the Iwasawa Main Conjecture for $GL_2$. In Thanasis Bouganis and Otmar Venjakob, editors, *Iwasawa Theory 2012*, volume 7 of *Contributions in Mathematical and Computational Sciences*, pages 35–61. Springer Berlin Heidelberg, 2014.

[23] L. Washington. *Introduction to Cyclotomic Fields*. Springer-Verlag New York, 1997.